

A Thesis Submitted for the Degree of PhD at the University of Warwick

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/98529>

Copyright and reuse:

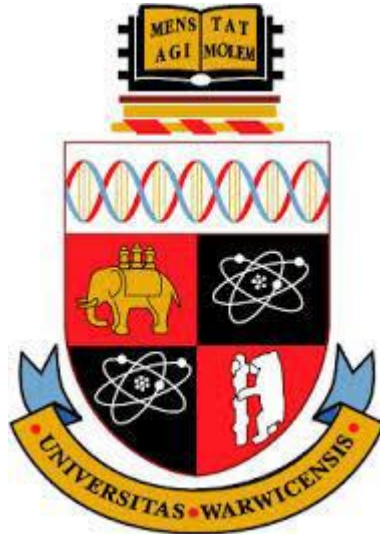
This thesis is made available online and is protected by original copyright.

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it.

Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk



Mobile Learning Security in Nigeria

By

Shaibu Adekunle Shonola

**A thesis submitted in partial fulfilment of the requirements for
the degree of**

Doctor of Philosophy in Computer Science

University of Warwick, Department of Computer Science

May 2017

Table of Contents

| Chapter | Page |
|---|------|
| Table of Contents | iii |
| List of Tables..... | viii |
| List of Figures | ix |
| Acknowledgements | xi |
| Declaration | xii |
| Dedication | xiv |
| Nomenclature | xv |
| Abstract | xvii |
| CHAPTER I | 1 |
| Introduction | 1 |
| 1.1 Background and Motivations | 1 |
| 1.2 Statement of the problem | 3 |
| 1.3 Research Questions and Objectives | 4 |
| 1.4 Structure of the thesis | 8 |
| 1.5 Publications in relation to this thesis | 11 |
| 1.6 Profile of the Case Studies | 12 |
| 1.6.1 University of Lagos (UNILAG)..... | 12 |
| 1.6.2 Lagos State University, Lagos (LASU) | 13 |
| 1.6.3 National Open University (NOUN) | 13 |
| 1.6.4 Yaba College of Technology (YABATECH) | 14 |
| CHAPTER II..... | 15 |
| Background and Literature Review | 15 |
| 2.1 Traditional Distance Education | 15 |
| 2.2 Modern Distance Learning Technologies | 16 |
| 2.2.1 E-learning Technology Overview | 17 |
| 2.2.2 M-learning Technology..... | 22 |
| 2.2.3 M-learning Devices | 27 |
| 2.2.4 Relationship between e-learning and m-learning..... | 29 |
| 2.3 Overview of Security Issues in E-learning and M-learning | 31 |
| 2.3.1 Security issues common to e-learning and m-learning systems (Database and Application Server levels) | 32 |
| 2.3.2 Security issues in e-learning and m-learning (Client level) | 35 |

| | | |
|---|--|----|
| 2.4 | M-learning Security Issues in Nigerian HEIs..... | 39 |
| 2.5 | M-learning in an alternative education environment | 41 |
| 2.6 | Summary | 43 |
| CHAPTER III | | 45 |
| Methodology | | 45 |
| 3.1 | Introduction | 45 |
| 3.2 | Overview of the Methodological Approaches..... | 46 |
| 3.2.1 | Document review | 46 |
| 3.2.2 | User-Centred Design (UCD)..... | 47 |
| 3.2.3 | Iterative Development and Implementation..... | 51 |
| 3.2.4 | User-centred Evaluation..... | 52 |
| 3.3 | Data collection methods..... | 53 |
| 3.3.1 | Quantitative | 54 |
| 3.3.2 | Qualitative | 55 |
| 3.3.3 | Case Study..... | 56 |
| 3.3.4 | Mixed method and triangulation | 57 |
| 3.4 | Sample and sampling technique | 58 |
| 3.5 | Data Analysis | 59 |
| 3.6 | Research Ethics | 60 |
| 3.7 | Summary | 62 |
| CHAPTER IV | | 63 |
| Users' Experience – Findings, Evaluation & Validation | | 63 |
| 4.1 | Introduction | 63 |
| 4.2 | Survey Questions..... | 64 |
| 4.3 | Methodology | 65 |
| 4.3.1 | Student Questionnaire Survey..... | 66 |
| 4.3.2 | Teachers' Interview..... | 67 |
| 4.4 | Pilot Study | 68 |
| 4.5 | Analysis of Results | 69 |
| 4.6 | Statistical and Hypothesis Testing | 78 |
| 4.7 | Discussion | 82 |
| 4.8 | Summary | 93 |
| CHAPTER V..... | | 95 |
| M-learning Attack Vectors..... | | 95 |
| 5.1 | Introduction | 95 |
| 5.2 | Threats to m-learning systems..... | 95 |
| 5.3 | Experimental Research Questions..... | 98 |
| 5.4 | Design of the study..... | 98 |
| 5.4.1 | Data Analysis | 98 |

| | | |
|---|--|-----|
| 5.5 | Results and findings | 99 |
| 5.6 | Discussion | 101 |
| 5.7 | Statistical and Hypothesis Testing | 104 |
| 5.7 | Limitations..... | 107 |
| 5.8 | Summary | 107 |
| CHAPTER VI | | 109 |
| M-learning Security Framework | | 109 |
| 6.1 | Introduction | 109 |
| 6.2 | Evaluating Existing Frameworks | 110 |
| 6.3 | General requirements for the security framework..... | 114 |
| 6.4 | Gathering and analysing the requirements | 117 |
| 6.5 | Architecture and design of the framework | 118 |
| 6.6 | The proposed framework..... | 119 |
| 6.6.1 | The main framework | 119 |
| 6.6.2 | Client Sub-framework..... | 122 |
| 6.6.3 | Server Sub-framework | 123 |
| 6.6.4 | Network Infrastructure Sub-framework..... | 125 |
| 6.6.5 | Discussion | 126 |
| 6.7 | Evaluation of the Framework | 127 |
| 6.7.1 | Aims | 127 |
| 6.7.2 | Design of the evaluation method..... | 128 |
| 6.7.3 | Analysis of the evaluation | 129 |
| 6.7.4 | Discussion | 131 |
| 6.8 | Summary | 132 |
| CHAPTER VII | | 134 |
| M-learning Security Enhancement app | | 134 |
| 7.1 | Introduction | 134 |
| 7.2 | Evaluation of existing security measures | 136 |
| 7.3 | Requirements, Design and Functionalities | 138 |
| 7.3.1 | The app Architecture..... | 139 |
| 7.3.2 | App Design | 141 |
| 7.4 | App Functionalities: How it works | 142 |
| 7.4.1 | Limiting unauthorised access..... | 143 |
| 7.4.2 | Avoiding malware attack | 144 |
| 7.4.3 | Learning Content Security | 145 |
| 7.4.4 | Free Wi-Fi Concern..... | 146 |
| 7.4.5 | Unusual Device Behaviour | 147 |
| 7.4.6 | Bluetooth Security Concern | 149 |
| 7.4.7 | Browsing Securely | 150 |
| 7.4.8 | Regular updates | 151 |
| 7.4.9 | Security Enhancement Report..... | 152 |

| | | |
|---|---|-----|
| 7.5 | The App Implementation..... | 153 |
| 7.6 | The App Evaluation..... | 154 |
| 7.6.1 | Aims | 154 |
| 7.6.2 | Design of the evaluation method..... | 154 |
| 7.6.3 | The Users’ opinons – Students..... | 156 |
| 7.6.4 | The expert opinions – Academic tutors | 158 |
| 7.6.5 | Comparing Interview and Questionnaire Results | 160 |
| 7.6.6 | The activity logs | 160 |
| 7.7 | Discussion | 162 |
| 7.8 | Recommendations from the evaluation..... | 164 |
| 7.9 | Summary: Link with Research Question..... | 165 |
| CHAPTER VIII..... | | 167 |
| Other M-learning Challenges in Nigeria..... | | 167 |
| 8.1 | Introduction | 167 |
| 8.2 | Methodology | 168 |
| 8.3 | The findings..... | 168 |
| 8.3.1 | Curriculum alignment | 168 |
| 8.3.2 | Excessive Reliance on Mobile Devices | 169 |
| 8.3.3 | Incompetency of Staff..... | 170 |
| 8.3.4 | Lack of Infrastructure..... | 171 |
| 8.3.5 | Inadequate Funding..... | 172 |
| 8.3.6 | Attitudinal Barrier | 172 |
| 8.3.7 | Regulatory Issues | 173 |
| 8.3.8 | Political and Legal Issues..... | 174 |
| 8.4 | Data Analysis of the study..... | 174 |
| 8.5 | Statistical and Hypothesis Testing | 176 |
| 8.6 | Recommendations | 177 |
| 8.7 | Summary | 179 |
| CHAPTER IX | | 181 |
| Summaries, Challenges, Contributions and Conclusion | | 181 |
| 9.1 | Introduction | 181 |
| 9.2 | Summarised Discussions from chapters..... | 182 |
| 9.2.1 | Discussion on user’s experiences..... | 182 |
| 9.2.2 | Discussion of the findings on security breaches | 182 |
| 9.2.3 | Discussion of the findings on m-learning security framework | 183 |
| 9.2.4 | Discussion of the findings on security enhancement app | 184 |
| 9.2.5 | Discussion of the findings on other challenges..... | 185 |
| 9.3 | Research Challenges, Scope and Limitations..... | 185 |
| 9.3.1 | Challenges | 185 |
| 9.3.2 | Scope | 186 |
| 9.3.3 | Limitations | 187 |

| | | |
|-------|---|-----|
| 9.4 | Research contributions and significant..... | 188 |
| 9.4.1 | Significance of research | 188 |
| 9.4.2 | Contribution to Knowledge..... | 189 |
| 9.4.3 | Dissemination of knowledge gained | 190 |
| 9.4.4 | Generalization of results | 191 |
| 9.5 | Conclusion and Future research | 191 |
| 9.5.1 | Suggestions for future research..... | 192 |
| | Bibliography..... | 193 |
| | Appendix 1 | 211 |
| | First Research Questionnaire | 211 |
| | Appendix 2..... | 221 |
| | First Research Interview | 221 |
| | Appendix 3..... | 227 |
| | Frameworks Interview | 227 |
| | Appendix 4..... | 229 |
| | Enhancement App Questionnaire..... | 229 |
| | Appendix 5..... | 233 |
| | Enhancement App Interview..... | 233 |

List of Tables

| | |
|--|-----|
| Table 2.1: A comparison of e-learning and m-learning..... | 29 |
| Table 2.2: Security issues in e-learning and m-learning (Client level)..... | 36 |
| Table 4.1 How important do students consider the security of their mobile devices..... | 77 |
| Table 4.2 Ranking of female and male on m-learning security..... | 78 |
| Table 4.3 Mann- Whitney test on m-learning security..... | 78 |
| Table 4.4 Ranking of female and male on m-learning security effects..... | 78 |
| Table 4.5 Mann- Whitney test on m-learning security effects..... | 79 |
| Table 4.6 Ranking of main stakeholders in m-learning security..... | 79 |
| Table 4.7 Mann- Whitney test on m-learning security threats..... | 80 |
| Table 4.8 Ranking of main stakeholders in m-learning..... | 80 |
| Table 4.9 Mann- Whitney test on main stakeholders..... | 80 |
| Table 5.1 What is the common attack route in m-learning system..... | 104 |
| Table 5.2 Has the security of your device been breached before..... | 105 |
| Table 5.3 Ranking of students and educators on security breach..... | 105 |
| Table 5.4 Mann- Whitney test on how the security of mobile devices are breached..... | 106 |
| Table 7.1. Gender/Age group demography..... | 155 |
| Table 7.2 Gender/Age Group of interview participants..... | 157 |
| Table 7.3 The app scan/check activity logs table..... | 161 |
| Table 8.1 ranking of dimension (students and educators) on the barriers of m-learning..... | 176 |
| Table 8.2 Mann- Whitney test on the barriers of m-learning..... | 176 |

List of Figures

| | |
|---|-----|
| Figure 4.1 How important students consider the security of their mobile devices..... | 69 |
| Figure 4.2 Security issues learners may encounter in m-learning..... | 70 |
| Figure 4.3 How the students are being affected by m-learning security threats | 71 |
| Figure 4.4 How educators are being affected by m-learning security threats..... | 73 |
| Figure 4.5 What are the m-learning security issues that stakeholders may face..... | 74 |
| Figure 4.6 How educational institutions are being affected by m-learning threats..... | 75 |
| Figure 4.7 The affected stakeholders in m-learning | 76 |
| Figure 5.1 Which component of m-learning is commonly attacked..... | 98 |
| Figure 5.2 How is the security of m-learning devices breached..... | 100 |
| Figure 6.1 Ramjan’s mLearning security conceptual framework..... | 113 |
| Figure 6.2 Proposed m-learning security framework..... | 120 |
| Figure 6.3 Mobile client security sub-framework..... | 122 |
| Figure 6.4 Server level security sub-framework..... | 123 |
| Figure 6.5 Network Infrastructure sub-frame..... | 125 |
| Figure 7.1 System diagram of the architecture of the app..... | 139 |
| Figure 7.2 The app flowchart..... | 141 |
| Figure 7.3 The app home page and activity list..... | 142 |
| Figure 7.4 The app password security check..... | 143 |
| Figure 7.5 The app list and permissions..... | 144 |
| Figure 7.6: The app learning content security..... | 145 |
| Figure 7.7 How the app Wi-Fi security..... | 146 |
| Figure 7.8 The app scanner service..... | 147 |
| Figure 7.9 The app scanner service II..... | 147 |
| Figure 7.10 Bluetooth Security..... | 148 |

| | |
|--|-----|
| Figure 7.11 Bluetooth Security II..... | 149 |
| Figure 7.12 Browsing Securely..... | 150 |
| Figure 7.13 Check OS update status..... | 151 |
| Figure 7.14 The app tips and enhancement report..... | 152 |
| Figure 7.15 How the app is useful to the participants..... | 155 |
| Figure 7.16 The features of the app..... | 156 |
| Figure 7.17 Users' opinions on the app functionalities..... | 157 |
| Figure 7.18 Users' opinions on the section of the app in terms of security..... | 158 |
| Figure 7.19 The app security features..... | 159 |
| Figure 7.20 The app functionalities and purpose..... | 160 |
| Figure 8.1 Barriers to m-learning adoption in Nigeria Universities..... | 170 |
| Figure. 8.2 Barriers to m-learning in Nigeria as highlighted by students and educators..... | 175 |

Acknowledgements

I would like to take this opportunity to thank everyone who supported and stood by me during the PhD study. I would like to begin with special thanks to my amicable supervisor, Professor Mike Joy for his advice, encouragement, supervision and reassurance throughout my programme. His advice and direction played a crucial role not only in successful and timely completion of this thesis but also in obtaining Associate Fellow of the Higher Education Academy. I truly appreciate for your mentorship. I would also like to thank my internal examiner Dr. Jane Sinclair, my advisors Dr. Alexandra Cristea and Steve Mathew for your constructive criticism and feedback on my research during the annual review viva. All your suggestions and feedback made valuable contributions to this thesis.

My special gratitude goes to Professor John Traxler for accepting the request to be the external examiner for my thesis. Many thanks to all my research participants in Lagos, Nigeria particularly Dr. Rasaq Kareem and Dr. Mutiu Rufai for your advice and active participation in data collection. Other people who deserve my appreciation include my colleagues in office CS327 and 329, doctoral colleagues in the University of Warwick, and my friends in the UK and in Nigeria especially Mr. Wale Adegayeye, Mrs. Titi Adegayeye and Mr. Ibrahim Owonikoko.

Special thanks to my wife, Lara Shonola for being my pillar of my strength. I appreciate and love you so much. And special thanks to my children, Ameerah, Adam, Aisha and Aryan for your understanding and giving me freedom to carry out this research.

Finally, I thank the Almighty God for everything and for making my wishes come true.

Declaration

I hereby declare that except where specific references are made to the work of others, the contents of this thesis are original, written by myself and presented in accordance with the regulations for the degree of Doctor of Philosophy. The research in this thesis has been undertaken by myself except where otherwise stated and has not been submitted in whole or in part for consideration for any other degree or qualification in any other University. Parts of this thesis have been published previously as follows.

Chapter four research on user' experience on m-learning security was published in two conference proceedings as follows: S.A. Shonola and M.S. Joy (2014), "Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)". 6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain. pp. 7081-7088; S.A Shonola and M.S Joy (2014), "Mobile Learning Security Concerns from University Students' Perspectives", 8th International Conference on Interactive Mobile Communication Technologies and Learning, November 13-14, 2014, Thessaloniki, Greece. pp. 165-172 and a much more detailed version was published in journal articles as follows: S.A Shonola and M.S. Joy (2014), Learners' Perception on Security Issues in m-learning (Nigerian Universities Case Study), Warwick Exchanges: The Warwick Research Journal, Vol. 2(1), October 2014, pp. 107 – 128 and S.A Shonola and M.S. Joy (2015), Security of m-learning System: A Collective Responsibility, International Journal of Interactive Mobile Technologies, iJIM – Volume 9, Issue 3, 2015, pp.64 – 70.

Extract of Chapter five on m-learning attack vectors was published in the conference proceedings: S.A Shonola and M.S Joy (2014), "Investigating Attack Vectors in M-learning Systems in Nigerian Universities". 8th International Conference on Interactive Mobile Communication Technologies and Learning, November 13-14, 2014, Thessaloniki, Greece. pp. 178-184. The framework in Chapter six was published in a conference paper as: S.A Shonola and M.S. Joy (2014), "Security

framework for mobile learning environments” A Proceeding of International Conference of Education, Research and Innovation (ICERI2014), 17th-19th November 2014, Seville, Spain. The proposed m-learning security model in Chapter seven has been published in journal article: S.A Shonola and M.S. Joy (2016), Enhancing Mobile Learning Security, International Journal on Integrating Technology in Education (IJITE) Vol.5, No.3, September 2016. An overview of the findings on other security challenges in Chapter eight have been published in conference proceedings: S.A Shonola and M.S. Joy (2014), “Barriers to m-learning in higher education institutions in Nigeria” A Proceeding of International Conference of Education, Research and Innovation (ICERI2014), 17th-19th November 2014, Seville, Spain.

Other publications in relation to the author’s research programme are listed in section 1.5 of the thesis.

Dedication

I would like to dedicate this thesis to my wife and children for their patience, support and understanding throughout my program of study.

And

To the memory of my parents and grandparents, you all live in my heart.

“To live in the hearts we leave behind is not to die” - Thomas Campbell

Nomenclature

| | |
|-------|--|
| AES | Adaptive Educational System |
| CS | Computer Science |
| DLI | Distance Learning Institute |
| GASSP | Generally Accepted System Security Principles |
| HEI | Higher Educational Institution |
| HTML | Hyper Text Mark-up Language |
| ICT | Information and Communications Technology |
| IS | Information System |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| LASU | Lagos State University |
| NOUN | National Open University of Nigeria |
| NUC | National Universities Commission |
| OU | Open University |
| PDA | Personal Digital Assistant |
| RAD | Rapid Application Development |
| SSADM | Structured Systems Analysis and Design Method |
| TAM | Technology Acceptance Model |
| UCD | Users Centred Design |
| UCE | Users Centred Evaluation |

| | |
|----------|--|
| UNESCO | United Nations Educational, Scientific and Cultural Organisation |
| UNILAG | University of Lagos |
| Wi-Fi | Wireless Fidelity |
| WML | Wireless Markup Language |
| XHTML | Extensible Hypertext Mark-up Language |
| XML | Extensible Mark-up Language |
| YABATECH | Yaba College of Technology |

Abstract

Innovation in learning technologies is driven by demands to meet students' needs and make knowledge delivery easier by Higher Education Institutions. The technologies could play an important role in extending the possibilities for teaching, learning, and research in higher educational institutions (HEIs). Mobile learning emerged from this innovation as a result of massive use in the number of mobile devices due to availability and affordability among students.

The lightweight nature of mobile devices in comparison to textbooks is also a source of attraction for students. Competition in the mobile device industry is encouraging mobile developers to be innovative and constantly striving to introduce new features in the devices. Consequently, newer sources of risks are being introduced in mobile computing paradigm at production level. Similarly, many m-learning developers are interested in developing learning content and instruction without adequate consideration for security of stakeholders' data, whereas mobile devices used in m-learning can potentially become vulnerable if the security aspects are neglected. The purpose of this research is to identify the security concerns in mobile learning from the users' perspective based on studies conducted in HEIs in Nigeria.

While the challenges of adopting mobile learning in Nigerian universities are enormous, this study identifies the critical security challenges that learners and other users may face when using mobile devices for educational purposes. It examines the effects on the users if their privacy is breached and provides recommendations for alleviating the security threats. This research also, after considering users' opinions and evaluating relevant literature, proposes security frameworks for m-learning as bedrocks for designing or implementing a secured environment. In identifying the security threats, the study investigates components of mobile learning systems that are prone to security threats and the common attack routes in m-learning, most especially among students in Nigerian universities.

In order to reduce the security threats, the research presents a mobile security enhancement app, designed and developed for android smart mobile devices to promote security awareness among students. The app can also identify some significant security weaknesses by scanning/checking for vulnerabilities in m-learning devices as well as reporting any security threat. The responsibilities of the stakeholders in ensuring risk free mobile learning environments are also examined.

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology — Bruce Schneier

A country that spends billions of dollars on cyber security every year couldn't secure a simple mail server- News extract on Americans e-mail hack by Russians.

However,

Security must be omnipresent throughout your infrastructure in order for you to begin to feel your application or service is secure

--C. Steel, R. Nagappan and Ray Lai

CHAPTER I

Introduction

1.1 Background and Motivations

The classroom offers an ideal learning space as it provides face-to-face communication between tutors and classmates. It is known to be a very structured means of passing knowledge, as classes can be scheduled in advance, thus making it easier to plan everyday tasks. Furthermore, it offers more physical interaction than any other methods by giving access to learning infrastructures, library and equipment, which undoubtedly improves the learning experience for the students (Djigic and Stojiljkovic, 2011). Advances in technology have made rapid changes to classroom teaching, and in most advanced countries, gone are the days when lecturers used blackboards from where the students copied lecture notes passively (Keser *et al.*, 2011). Nowadays, technologies have aided learning by the introduction of projectors, laptops, white and intelligent boards to classrooms. The addition of these technologies into classrooms as teaching and learning aids has been step-wise. Lecturers and instructors also generally appreciate how these modern learning technologies can be effectively and efficiently used to enhance their method of teaching (Kukulska-Hulme *et al.*, 2009).

However, the cost of equipping and running classrooms as well as the supporting facilities is ever increasing. The costs are normally passed to the students being taught in these classrooms as a bulk part of their tuition fees (Ibrahim *et al.*, 2011), but everyone may not be able to afford these expensive fees, and there is a need to run a less expensive method of education. Many distance learning and e-learning programmes being run by universities in the UK appear to be relatively cheaper than campus based programmes. Distance learning and e-learning platforms have enhanced the delivery of education through flexibility, a comfortable environment,

online group interaction, and by offering a short interval of study (Beauchamp and Kennewell, 2010). Outside the university learning environment, communication equipment such as mobile devices are making changes to the ways learners get information and how they learn. The effect of these changes is a new approach to learning and education which is very different from the static classroom structure (Ally and Prieto-Blázquez, 2014). Mobile learning is being integrated into distance and e-learning programmes to provide a complete package of virtual education. As modern information and communications technologies have changed the world immensely in the last two decades, many aspects of human life are going mobile and mobile applications are being used in banking, trading, travels, and businesses, as well as in education as a learning tool in advanced countries.

Mobile technology is a fast growing and developing industry in Nigeria with about two-thirds of the population using smart phones (that is about 100 million people out of 150 million population). While the Nigerian government is putting in place several initiatives to encourage Information Technology and Communication (ICT) studies, there are inadequate numbers of universities to implement these good initiatives. According to the website of National Universities Commission (NUC), there are fewer than 155 universities in the country serving the large population (NUC, 2012). Ironically, many of these institutions are only delivering classroom based programmes and they are engaging desktop computers as their main teaching and research equipment. Although e-learning is a known term within the education sector, it is still a growing form of knowledge delivery in Nigerian Universities and it faces many difficulties such as funding, high cost of software and erratic power supply (Aboderin, 2015).

There is a huge demand for some other forms of education delivery, most especially mobile learning, which is still at an early stage in the country. Research efforts and development are needed to implement mobile-learning successfully. Nigeria like many other developing countries face a lot of issues in using mobile technologies as

educational tools. There are numerous problems in the existing learning system in Nigeria such as poor infrastructure development and lack of instructional materials that inhibit the ability to properly implement mobile learning solutions. Security challenges of m-learning are also becoming increasingly significant as more universities in the country are deploying mobile technologies to augment their education delivery. Research efforts are also needed to study various security issues concerning the use of mobile learning in higher educational institutions in Nigeria. This will ensure the delivery of suitable education materials to learners at the right time and also prevent unauthorised access to materials they do not need. This research study is, therefore, focused on the security issues being encountered for successful implementation and acceptance of mobile learning in higher institutions in Nigeria. It will identify all possible security threats a higher institution will face in deployment of mobile learning along with conventional ways of teaching and how to overcome those threats. In addition, the study will highlight the prospects and tangible benefits of delivering secured mobile learning in higher institutions in developing countries. Apart from security aspects of mobile learning, this research briefly reviews other challenges affecting successful adoption of mobile learning in Nigeria such as lack of technical expertise, social, pedagogical and political challenges (Oyelere *et al.*, 2016).

1.2 Statement of the problem

Until recently, stakeholders in HEIs in Nigeria were unconcerned about security, mainly because users in academic fields were assumed not to be malicious. However, security in any learning environment is becoming vital as online learning system and infrastructure have become ‘business-critical’ applications in HEIs. Therefore, stakeholders, most especially the University management and academic staff, are now seeing security issues in learning technologies as a part of the overall educational and business strategy of their institutions. Mobile devices, like any other technology, have

inherent risk and security issues, which are being transferred into the learning environment as a result of m-learning. While some lecturers use mobile technology as a teaching aid, many students use their mobile device as a learning tool without adequate consideration for related security issues. Due to these security threats, user confidentiality, integrity and data availability are at stake.

Mobile devices are now targets for hackers because of their extensive use (Kambourakis, 2013), and this causes higher education institution management, educators, and individual learners to be profoundly worried about the growing security threats in m-learning. Protecting learning contents, instruction and assessment results against manipulation is necessary and important (Luminita and Magdalena, 2012), particularly in Nigeria which was ranked sixth in internet security threats and web based attacks (Chidiogo, 2013). The security aspect of mobile learning is becoming increasingly important as more universities are deploying mobile technologies to complement their classroom learning delivery, and the users in the HEIs (that is education providers, educators, mobile learning developers and promoters) should be concerned about the security implications of these devices in teaching and learning environments. By performing a systematic analysis of the risks inherent in mobile devices, vis-à-vis learning, specific security issues relating to mobile learning can be addressed and resolved. It is in-line with this background that this study is being carried out to determine the security issues that are affecting the use of mobile devices for learning and to identify possible strategies to overcome security concerns in the implementation and deployment of mobile learning in HEIs in Nigeria.

1.3 Research Questions and Objectives

In finding solutions to the m-learning security issues and threats, the following research questions were drawn up from the study motivations and statement problem

described in the sections above. Research objectives and sub-research questions are then drawn for and from these main research questions respectively. Some of the research questions are peculiar to the Nigeria learning environment while some are general and applicable to m-learning anywhere around the world.

RQ 1: What are the threats to m-learning in HEIs in Nigeria?

This broad research question is formulated to identify the security threats to m-learning in Nigeria. It identifies the prevalent issues through a literature review and the research surveys we conducted. These investigations reflect the current events, as well as the significant challenges, in the area of study. Thus, the research objectives here are as follows.

1. To perform research on, and investigates m-learning security challenges, understand the research area in-depth, to critically review and analyse current research papers and literature on m-learning security, particularly in Nigeria, and to produce up to date information of interest to stakeholders.
2. To gather up to date data and ideas that are relevant to the project and ensure that the research is conducted based on established research methodologies.

The followings are the survey questions to the first main question.

- What possible security threats can a higher education provider face in deployment and use of mobile learning technologies along with conventional methods?
- What are the prevalent m-learning security issues in HEI in Nigeria?
- Which components of m-learning systems are commonly attacked (mobile devices, servers or network devices)?
- How is the security of m-learning devices breached in Nigerian universities?

RQ 2: What are the users' experiences on m-learning in HEIs in Nigeria?

This research question focuses on the users of m-learning in Nigeria who are mainly the students and academic staff. The question was designed to obtain their experiences on the security challenges through research surveys that were carried out in the HEIs used as case studies. The research objectives are the following.

3. To investigate the security and privacy issues that stakeholders are encountering, or likely to encounter, when using mobile devices in education.
4. To identify possible security threats a higher education institution will face in deployment of mobile learning along with conventional ways of teaching, and how to overcome them.
5. To analyse the result of the investigation and report on major findings on factors affecting the m-learning security.

The followings are the (survey) questions that are formulated from, and used to answer, the second research question.

- How important do students consider the security of their mobile devices and what concerns do they have when using their devices for learning?
- What are the lecturers' concerns on security issues in m-learning in Higher Education Institutions in Nigeria?
- How are the education providers and other stakeholders being affected by the security threats in m-learning, and who among these stakeholders are most affected by the security issues?
- What are the responsibilities of the stakeholders in ensuring risk free m-learning?

RQ 3: How can an m-learning security framework and m-learning enhancement app be used to reduce the threats?

This research question aims to study the technical components of our solution to m-learning threats, the m-learning security enhancement app. In order to alleviate the threats in an m-learning environment, we present m-learning security framework and m-learning enhancement app as our interventions. The proposed framework serves as a pillar for designing a secured m-learning environment while the enhancement app is a simple user app developed to enhance the inbuilt security of m-learning devices, and which their effectiveness was evaluated from the user perspective in this thesis. The objectives of from this research question are the following.

6. To identify solutions and to develop an app that captures m-learning vulnerabilities.
7. To review the whole project and identify possible future opportunities and enhancements on this research and to come up with recommendations for future work.

The survey questions that are designed to answer the main research question are as follows.

- How can the security issues and threats be assessed in Nigerian HEIs?
- How can the security issues and threats be reduced in Nigerian HEIs?

RQ 4: How is the m-learning security enhancement app evaluated?

This research question investigates the manners in which the security enhancement app that was developed as an intervention to some of the m-learning security issues was evaluated using quantitative and qualitative measures as well as case study and logging of users' activities.

RQ 5: What are the other m-learning challenges that exist in the Nigerian education sector?

This research question investigates other challenges being faced by providers or educational institutions when adopting m-learning in Nigeria, apart from security issues, in order to provide a comprehensive solution package. The research objective is

8. To investigate other barriers facing mobile learning in Nigeria such as political and legal challenges.

The sub-research (survey) questions that are designed to answer the main research question are as follows.

- What other threats, such as political and legal, are facing mobile learning in Nigeria?
- What are the recommendations for addressing these challenges in Nigeria?

1.4 *Structure of the thesis*

Chapter one is the opening chapter of the thesis, starting with the background of the whole research work, it gives the rationale for the study and structured problem statements about security issues in m-learning and the motivation for doing the research. It also outlines the main research questions which are the backbone of the study and the objectives to be achieved after finding solutions to the questions. The chapter concludes by highlighting the author's publications in relation to the research. Chapter two starts with the review of traditional distance learning and also evaluates past and current developments in the modern learning environments, in particular e-learning and m-learning, making comparisons between the learning platforms. An overview of the security, privacy and trust issues in these learning systems was carried out. This chapter further identifies gaps and problems in m-learning within

Nigerian higher educational institutions, hence provides motivation to conduct this research.

Chapter three discusses the research activities on which the studies in this thesis were conducted. It gives detail on the research methodology which was adopted to establish the answers to the research questions, and in particular the data collection methods. It gives an overview of the research design, sampling methods, and brief details about the participants. Mapping of the research methods to the objectives is highlighted and the chapter concludes with ethical issues and a summary. Chapter four discusses the security threats in m-learning systems and determines which components of mobile learning system are prone to attack and also what are the common attack routes in Nigerian university environments using both quantitative and qualitative methods. The quantitative findings were validated using Mann-Whitney statistical tests. Recommendations on how to reduce the attacks on m-learning systems are also highlighted. Chapter five explores the user experience on security issues in m-learning, starting with the academic tutors to students and other stakeholders such as the managers of the education institutions and non-teaching staff. The chapter gathers data from the largest number of participants, analysing their experiences using quantitative and qualitative methodologies. The results obtained were validated using chi-square and Mann-Whitney U tests. Recommendations on how to overcome or reduce the identified issues are also discussed.

Chapter six presents a designed proactive m-learning security framework which acts as a suggestion mechanism to tackle security and privacy concerns. The proposed mobile learning security framework, which follows Generally Accepted System Security Principles (GASSP) and Technology Acceptance Model (TAM) that can be used to help detect and deter security and privacy issues. The framework presents a three-layered systems development approach. It highlights the issues to contemplate when developing security applications to support m-learning and presents security

content and activity to enhance security in m-learning. The evaluation of the framework from the perspective of the teachers as experts who teach computer related courses was done using qualitative analyses in order to establish if the ideas proposed by the framework are appropriate and fit for purpose.

In chapter seven, we present a mobile security enhancement app as an intervention designed and developed for Android smart mobile devices in order to promote security awareness among students. The app can also identify most major and significant security weaknesses and scan or check for vulnerabilities in m-learning devices as well as report any security threat. The chapter also describes the app requirement, architecture and functionalities. The chapter evaluates the enhancement app by conducting a case study with HEIs students and tutors in Nigeria Universities. The chapter describes how the users interact with the app through installing, accessing the app functionalities and performing some security activities on their devices with the app. The tutors provide evaluations as experts while the students provide the users' opinions of the app in order to establish whether use of such an app is effective in reducing the security threats.

Chapter eight describes other barriers to m-learning in Nigeria apart from the security issues, such as lack of technical expertise, infrastructure and attitudinal challenges. It gives detailed explanation on barriers which were established through the research study. Validation of the study was done using standard statistical tests. The chapter concludes by giving recommendations on overcoming the barriers. Chapter nine concludes the thesis and summarizes the discussion of the research project while also reflecting on the research limitations. The chapter also lists challenges encountered during the research activities. Also included in the chapter are the main contributions of this project to the research field, amongst these are the framework and the security enhancement app as an intervention. The final section outlines future research directions that could both improve and further the ideas embodied in this work.

1.5 Publications in relation to this thesis

- (a) S.A. Shonola and M.S. Joy (2014), “Mobile learning security issues from lecturers’ perspectives (Nigerian Universities Case Study)”. 6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain. pp. 7081-7088.
- (b) S.A Shonola and M.S Joy (2014), “Mobile Learning Security Concerns from University Students’ Perspectives”. 8th International Conference on Interactive Mobile Communication Technologies and Learning, November 13-14, 2014, Thessaloniki, Greece. pp. 165-172.
- (c) S.A Shonola and M.S. Joy (2014), “Security framework for mobile learning environments” A Proceeding of International Conference of Education, Research and Innovation (ICERI2014), 17th-19th November 2014, Seville, Spain
- (d) S.A Shonola and M.S. Joy (2014), “Barriers to m-learning in higher education institutions in Nigeria” A Proceeding of International Conference of Education, Research and Innovation (ICERI2014), 17th-19th November 2014, Seville, Spain
- (e) S.A Shonola and M.S Joy (2014), “Investigating Attack Vectors in M-learning Systems in Nigerian Universities”. 8th International Conference on Interactive Mobile Communication Technologies and Learning, November 13-14, 2014, Thessaloniki, Greece. pp. 178-184.
- (f) S.A Shonola and M.S. Joy (2015), “Security issues in E-learning and M-learning Systems: A Comparative Analysis” A Proceeding of 2nd WMG Doctoral Research and Innovation Conference (WMGRIC2015) 30th June – 1st July 2015, Warwick United Kingdom
- (g) S.A Shonola and M.S. Joy (2014), Learners’ Perception on Security Issues in m-learning (Nigerian Universities Case Study), Exchanges: The Warwick Research Journal, Vol. 2(1), October 2014, pp. 107 – 128.

- (h) S.A Shonola and M.S. Joy (2015), Security of m-learning System: A Collective Responsibility, International Journal of Interactive Mobile Technologies, iJIM – Volume 9, Issue 3, 2015, pp.64 – 70.
- (i) S.A Shonola, M.S. Joy, S. S. Oyelere and J. Suhonen (2016), The Impact of Mobile Devices for Learning in Higher Education Institutions: Nigerian Universities Case Study, Accepted for publication by International Journal of Modern Education and Computer Science (IJMECS)
- (j) S. S. Oyelere, J. Suhonen S.A Shonola and M.S. Joy (2016), Discovering Students Mobile Learning Experiences in Higher Education in Nigeria, Accepted for presentation and publication by Frontiers in Education Conference, USA.
- (k) S.A Shonola and M.S. Joy (2016), Enhancing Mobile Learning Security, International Journal on Integrating Technology in Education (IJITE) Vol.5, No.3, September 2016.

1.6 Profile of the Case Studies

In this section, we give a brief description of the four universities used as case studies namely; University of Lagos (UNILAG), Lagos State University (LASU), National Open University (NOUN) and Yaba College of Technology (YABATECH). All the four institutions are overseen and accredited by the relevant education boards in Nigeria.

1.6.1 University of Lagos (UNILAG)

According to the university website, The University of Lagos is among the first generation of universities in Nigeria established in 1962. It is a federal government funded university having fourteen academic units comprising many professional faculties, schools and departments. In addition to various departments in its faculties, the university also has other centres and institutes such as the Distance Learning

Institute (DLI). The University of Lagos offers many academic programs for undergraduate and postgraduate studies and it is known as a centre for academic research. The University is located in Akoka, Lagos mainland, South West Nigeria and it has a population of 57,000 students and 1,123 academic staff as of 2013. The department of computer science where some of this research work was carried out is one of ten departments in the faculty of science with an annual intake of around 200 students. The website of the university is www.unilag.edu.ng.

1.6.2 Lagos State University, Lagos (LASU)

Lagos State University was established in 1983 for the advancement of learning and establishment of academic excellence, according to the information gathered from the institution website. The university which is a state government owned educational institution caters for a population of over 60,000 students who enrolled for either full-time and part-time programmes. The university offers courses at Diploma, Undergraduate and Postgraduate levels. Lagos State University is located in Ojo, a town in Lagos State, South West Nigeria. LASU is the only state university in the former British colony. The university has nine faculties and about 80 departments. The department of computer science where some of this research work was undertaken was established in 2006 to meet the growing needs for computer experts in Lagos and Nigeria, is one of ten departments in the faculty of science with an annual intake of around 220 students. The website of the university is www.lasu.edu.ng

1.6.3 National Open University (NOUN)

The National Open University of Nigeria is the only federal government funded Open and Distance Learning institution, based on the information obtained from university website, it is the first of its kind in the West African countries. The university was initially established in 1983, suspended a year later and resuscitated in 2001. The National Open University of Nigeria operates an administrative head office in Lagos

and many study centres around the country. It offers over 50 academic programs and 750 courses to about 57,759 as of 2011. A diverse range of students from all walks of life are attracted to the National Open University of Nigeria just like other prominent Open Universities such as the Open University (OU) in the United Kingdom. The Open University is of importance to this research because it has a technological platform called NOUNiLearn as an online tool for education delivery and e-Courseware as an online library for downloading books and course materials. Study tools such as the Smart e-book Digitized lecture video and audio materials for an enhanced student' learning experience are available on the platform. Regular online class discussions are organised by the university facilitators thereby creating a virtual classroom environment for their students. The university administers the Computer-Based-Test form of examination to its students in their first and second years. The website of the university is www.noun.com.ng

1.6.4 Yaba College of Technology (YABATECH)

Yaba College of Technology, or YABATECH, is one of the Nigeria's first higher educational institutions founded in 1947. It is located along the coastal area of Lagos State, South West Nigeria, and has students' enrolment of over 16,000 and the total staff strength is about 1,600. According to the institution's website, the institution was established to provide full-time and part-time courses of instruction and training in technology, applied science, commerce and management, agricultural production and distribution; and for research. Yaba College of Technology is structured into eight schools and thirty-four academic departments with a total of sixty-four accredited programmes, which cut across the National Diploma (ND), Higher National Diploma (HND) and Post-HND Levels. It also offers B.Sc (Ed) courses in Technical and Vocational Education and Post Graduates Diploma in Engineering. Recently, the federal government of Nigeria granted the institution a university statute and it is still in the process of full conversion. The institution's website is www.yabatech.com.ng

CHAPTER II

Background and Literature Review

2.1 Traditional Distance Education

Alternative classroom learning methods can be traced back to traditional distance learning- a paper-based correspondence education. Along with classroom lectures, Universities around the world have been experimenting with other learning environments to accommodate the needs of their students, by providing correspondence courses, courses on tape, televised courses, and most recently internet based distance education or e-learning (Ferriman, 2013). Distance learning programs are basically designed to serve as off-campus study to students and these programs provide access to higher education for learners who cannot attend classroom lectures due to personal commitments, distance, employment and other expenses normally incur with classroom learning (Pappas, 2013).

The traditional distance learning approach also provides a cost-effective means to serve huge numbers of learners regardless of their location. The first generation of distance learning involved sending printed material and instructions via post to the students and communication with tutors through telephone while the second generation distance learning comprised audio recordings and radio broadcasts (Miller, 2014). Televised and taped recorded classes for students who cannot attend classes in lecture halls were offered by some universities and the recorded lectures were often placed in libraries for students' revision, this convenience gave some students an opportunity to choose either to attend classes for lectures or listen to the lectures at a later time (Hein, 2014). **Sending correspondence to students in form of recorded tapes and printed materials as identified by Ferriman (2013) and Hein (2014), was the beginning of modern day distance learning in Nigeria HEIs. However, this was only possible for students living cities and not those living in outside cities as there were not posted services in countryside.**

2.2 Modern Distance Learning Technologies

Over the years, distance learning has benefitted from developments in computing systems as well as information and communication technology (ICT). **Using technology in modern classrooms is now a trend in educational environment especially at the tertiary levels. Technology-rich learning environments can engage learners by giving them a sense of empowerment, in which they study in a community that is guided by teachers or instructors with the aid of technology. Technology has enhanced the two-traffic way of education as students can contribute to the process of pedagogical revolution that includes real-world presentation of ideas using latest online techniques.** Thus, the innovative technology has enabled distance learning to change into the conventional modern learning approach which is a form of digital electronic platform for passing knowledge and instruction from lecturers to learners, which mainly comprises of e-learning and m-learning. E-learning platforms have made delivery of education easier for learners by adding flexibility and convenience as well as easing information dissemination and achieving higher grades (Alsaaty et al., 2016). **As pointed out by Alsaaty et al. (2016), many HEIs in Nigeria are now incorporating e-learning as a form of knowledge delivery.**

The advent of mobile device technologies and maturity in e-learning, has given an impetus for mobile-learning (m-learning) to be integrated into traditional distance learning and e-learning curricula to form a complete package of virtual education (Ozuorcun and Tabak, 2012). **In Nigeria HEIs, online or digital education has therefore produces opportunities for creating an educational environment that improves the style of old environment and focuses on providing more information, optimizing the educational process and improving the effect of education. Students can pick the information by themselves through the digital medium. Educational technologies include digital presentation of educational content, in which information is presented using white boards, images,**

animation, and virtual classroom (Agbatogun, 2013). Furthermore, digital technologies are infused into the instructional process to bridge the gap between theoretical and practical knowledge. The use of these modern learning technologies in education introduces new threats to the learning environment such as security and privacy issues.

2.2.1 E-learning Technology Overview

There are many **descriptions** of e-learning that are given in the literature. **Carliner and Shank (2016) describe e-learning as a method of engaging Information and Communications Technology (ICT) devices and computer systems to deliver instruction, information, and learning content to students.** Ozuorcun and Tabak (2012, pp.3) describes “E-learning is the delivery of teaching materials via electronic media, such as the Internet, intranets, extranets, satellite broadcast, audio/video tape, interactive TV and CD-ROM”. **Therefore,** e-learning is being regarded as an electronic medium for passing knowledge from the instructor to students as well as a medium to facilitate information dissemination among learners. It is a modern form of education delivery via electronic media to boost the learner’s knowledge and learning skills.

The boom in ICT and dot com in the last two decades has given more acceptability to e-learning, Universities and higher education administrators are taking advantage of the innovation in ICT to design and offer new education packages for teaching and learning through the web which is used to supplement face to face learning (Allen and Seamans, 2011). **E-learning packages have been developed around the world and according to a 2011 report, over 6.1 million students were taking at least one e-learning course in 2010, with 31% of all students in higher education institutions taking at least one online course (Alsaaty et al., 2016). In another article, the number of students taking at least one e-learning course is approximately 570,000 in a million students. The article further states that while the number of students taking at least one e-learning course is at its highest level**

with a growth rate of 9.3 percent, there is no evidence that the trend will slow in the near future (Allen and Seamans, 2013).

Apart from the economic benefit, revenue generation and a large student base, e-learning has huge potential growth and provides many advantages to the stakeholders in the education sector who include instructors, students, university administrators, technical and support staff, and funding bodies. According to **Curran (2004, pp.1)**, “e-learning strategies adopted by universities have been approaching the core issue from three common objectives, which are (i) widening access to educational opportunity, (ii) enhancing the quality of learning and (iii) reducing the cost of higher education”.

E-learning is sometimes cheaper for learners than classroom based learning and less expensive to run by education providers. It appears to reduce classroom and facilities costs, travel costs, labour and other overhead costs for students. Carliner and Shank (2016) state that e-learning offers a potential saving over classroom training. However, e-learning also requires substantial investments in technology in terms of hardware cost, software licenses, material development, infrastructure maintenance and staff training and it may not save cost when compared to classroom learning.

All the sources above gave the benefit of e-learning in international context, which are also relevant to Nigeria HE. Furthermore, the benefits of e-learning claimed by researchers from Nigeria include accessibility to information, consistent content delivery, effective knowledge passage, personalized instruction, content standardization, individual self-pacing, improved collaboration and interaction (Aboderin, 2015; Osang et al., 2013).

Whilst all the above stated objectives and benefits being reaped in developed countries with the help of advanced technologies, one of the main objectives of e-learning in many developing countries is to provide necessary education to students at

a cheaper rate (Arkorful and Abaidoo, 2015). While many developing countries have expressed an interest in, and are starting to implement e-learning, it is still at an early stage and its implementation faces obstacles such as insufficient funding, poor infrastructure and technology, technical resources, lack of adequate support from institutions, inadequate legal backing from government, poor policy development and monitoring, and cultural barriers (Nawaz, 2013). **Most of the m-learning obstacles mentioned by Nawaz (2013) were relevant to m-learning in Nigeria and were similar to those being encountered by HEIs in Nigeria.**

According to Clark and Mayer, (2016) education through e-learning methods could be classified into synchronous and asynchronous learning. The classification also includes online support and knowledge databases. Synchronous learning occurs real-time, in which the instructor and learners are present virtually at the time of learning content delivery. Students log in at a pre-arranged time and communicate with the instructor and with one another. They can also (for example) raise cyber hands during lectures and view a whiteboard. Typical examples of synchronous learning environment are via internet sites, audio- or video-conferencing, and internet telephony. In asynchronous learning, the lecturer and students are not present at the time of content delivery. There is a good interaction among students and the instructor through discussion boards, email exchanges and online blackboards (that is posting of lecture notes and assignments online). A knowledge database in a self-paced hypermedia based learning environment is where learners receive the content media, along with step-by-step instructions for performing specific tasks and study at their own space and time. Learning materials could be recorded on a medium like CD ROM and DVD. It could also be delivered via intranet, internet or the web. Learning could be moderately interactive aided by step-by-step instructions for performing specific tasks with links to reference materials (Ramakrisnan *et al.*, 2011). Online support is part of an e-learning package which offers learners help and advice in the form of (for example) forums, chat rooms, live instant-messaging, discussion groups and tutorials. It gives the chance for more specific questions to be asked with

immediate answers (Ramakrisnan *et al.*, 2011). These techniques of e-learning can change the approaches in teaching and learning and serve as a viable alternative to classroom education. They encourage motivation and provide new ways of learning and thinking among students. The effectiveness and efficiency of e-learning create innovative methods to deliver instruction through a virtual environment.

Recent developments are transforming teaching strategies in e-learning with extra focus on students and their needs. Additional attention is given to individual learning objectives to make e-learning more effective and efficient than other methods of knowledge delivery. Current trends in modern e-learning education and teaching include adaptive e-learning, personalised learning, games as learning tools (Arkorful and Abaidoo, 2015). Adaptive e-learning is an emerging topic with the aim to develop learning content based on the needs of a particular learner. Brusilovsky states that modern e-learning systems should be clever to integrate different learning content that could be specifically adapted to individual knowledge of the subject, to enable full participation and interaction of the learner in the learning process. He further states that the e-learning navigation space should be suited to respond to the actual learner's need by limiting browsing space, suggesting relevant links and providing adaptive comments. The e-learning systems that are developed and built to integrate the changing individual user's needs are known as Adaptive Educational Systems (AES). The AES are able to deliver personalised views of documents based on a user model and a perceived model of the learning environment. The two models are used to make decisions on the contents and navigation space to give to the learners and how best to view the contents (Kim *et al.*, 2013).

Adaptive Educational Systems not only provide for the need of each individual learner, adapting to their learning goal, knowledge level, educational contexts, preferences and learning styles (Kim *et al.*, 2013), but also structure the contents to facilitate instruction and information dissemination to the specific user. During the development of AES, a user model is designed with some parameters which are

determined by assessing the needs, interests and problems of the user. While most systems use deterministic parameters such as age, personal attributes, and previous knowledge, many systems use cognitive models like learning styles or educational strategies. The challenges of the AES are getting the user model parameters and making the configuration in real time.

Another new development in e-learning is the change brought by the advent of Web 2.0 technologies, which focus on people interactions and collaboration within a community. Web 2.0 technology has the prospective to provide students with personalised learning activities according to students learning styles and gives learning experiences that are personally meaningful, collaborative, and socially relevant (Kurilovas and JUŠKEVIČIENĖ, 2014). Web 2.0 applications which include blogs, wikis, social media or social networking sites, allow a learner to interact with other learners, gain from one another experience and develop their own knowledge. According to Kaplan and Haenlein (2010), social media comprise of internet-based applications which are built on the ideological and technological fundamentals of Web 2.0 and they also permit the creation and exchange of user-generated content.

The emergence of Web 2.0 came along with e-learning 2.0. While Web 2.0 technologies use social media for socializing and connecting friends, family and collaboration within a social community, e-learning 2.0 caters for the educational aspect, and it is an improvement on the previously known e-learning platforms. Rather than essentially receiving, reading, and responding to learning content in a conventional e-learning environment, e-learning 2.0 permits learners to create content and to collaborate with group peers to form a learning network with delivery of content creation and responsibilities (Wu and Zhang, 2014). Furthermore, it makes use of different source of content aggregation into learning experiences and a variety of tools such as online references, courseware, knowledge management and collaboration.

As e-learning gains acceptability and maturity, m-learning emerges. M-learning is considered as an integral part of, and a derivation from, e-learning (Ozuorcun and Tabak, 2012). The next section discusses m-learning in detail. Although m-learning and e-learning are closely related and share many similarities, there are still some distinctions between the two platforms. E-learning is considered to be “tethered” (connected to something) and presented in a formal and structured way. In contrast, m-learning is usually self-paced, un-tethered and mostly informal in presentation. Mobile learning can be thought of as mobile devices integrated with e-learning, so that the mobile technology will provide benefits for students in studying both inside and outside the classroom, allowing access to course materials and interaction with their teachers and classmates through websites and mobile apps.

2.2.2 M-learning Technology

The application of computer and information devices is a force to be reckoned with in modern education systems which predominantly use e-learning. With the advent of emerging mobile technologies and its widespread usage as well as maturation in e-learning, the need to integrate mobile devices in learning is inevitable. Mobile learning emerges as a new progression and idea, based on the use of mobile devices together with wireless communications devices (Wu *et al.*, 2012).

There are many definitions of mobile learning, and the definitions theme around mobility and learning. Mobile learning refers to the delivery of educational material through mobile devices, such as personal digital assistants (PDAs), iPods, mobile phones, and smartphones, often believed to be a combination of PDAs and mobile phones (Pegrum, 2014). Furthermore, Behera, (2013) state that mobile learning is learning by means of wireless technological devices that can be pocketed and utilised wherever the learner is on the move. Paolucci (2014) describes mobile learning as a subset of e-learning that focuses on learning across various educational contexts using mobile devices (the application of small, portable, and wireless computing and

communication devices). The author stated that the main features of mobile learning are: its ability to provide learning that is just-in-time, learning that is situated (which typically occurs in the field or at the workplace); and learning that is contextualized through mediation with peers and tutors.

In line with these definitions, many researchers view mobile learning as the ability to deliver learning on mobile devices. The main focus of m-learning is using the massive development in mobile technologies to utmost advantage of the learners, improving the learning process and shortening the learning curve (Kearney *et al.*, 2012). **According to a researcher from Nigeria, m-learning, being a new innovation can be a modern avenue for training, teaching, learning and knowledge exchange without distance barrier (Okeke and Umoru, 2012).** Another focal point of m-learning is information sharing, which makes it possible for learners to interact with each other and share knowledge anytime anywhere.

M-learning is creating a new environment for teaching, learning and researching. While educators are using mobile devices as teaching aids, students are using them as learning tools. Academic researchers are also using their portable gadgets for collaboration. Lecturers can give out lecture notes and instructions while on the move and students can listen to recorded lectures either online or offline anytime anywhere. It allows learners to communicate with lecturers and peers, as well as access learning content and resources, while on the move (Traxler and Vosloo, 2014). M-learning therefore, extends learning beyond lecture theatres and can be made to support modern classroom teaching tools. Assessments can be done via mobile devices and feedback can be obtained through them. Therefore, one of the advantages of m-learning is that it gives learners a degree of freedom and independence in the course of learning (El-Hussein and Cronje, 2010). Another advantage of mobile learning is information sharing and collaboration, which makes it possible for research students to interact with each other and share knowledge and research outcomes anytime. Thus, students who use mobile technologies for learning are not only closer to their

lecturers and tutors, but also in full control accessing learning content and instructions through their mobile devices. This undoubtedly makes learning an exciting experience for the students and teaching a very interesting career for the lecturers. These advantages of m-learning are making many education institutions, providers and managers to focus on developing and delivering m-learning learning content. They can also align their educational curricula to accommodate m-learning and they are investing on hardware and software resources to take full advantage of the new technology.

Furthermore, m-learning provides an opportunity for personalised learning and it is characterised with the fact that learning can be done at any place and at any time whenever the student wants to study whether in the classroom, home or in transit (Ozuorcun and Tabak, 2012). It also serves as a medium that allows individuals to combine work, study and leisure together in meaningful ways. In addition, m-learning promotes collaborative learning, extends learning beyond lecture theatres and can be made to support modern classroom learning tools as well as distance learning and e-learning (Chaka and Govender, 2017). Knowledge acquisition through m-learning has neither boundary nor barrier in term of distance and space, thereby achieving the globalisation objective (Hashemi *et al.*, 2011). The possibilities of the tutors and the education providers to offer students services, learning instruction and information outside the traditional learning environment is becoming more suitable in education and learning due to the use of modern information and communication technologies such as mobile learning (El-Hussein and Cronje, 2010).

In Nigeria HEI context, Olugbenga (2015) indicated that m-learning offer new opportunities for students' educational activities in that they can be used across different locations and times and as a cost effective option for students in HEIs. Students who use mobile technologies for learning are not only far away from their lecturers and instructors, but they are also in full control of the access to information on their mobile devices. Therefore, a key importance of mobile learning is that it

gives learners certain amount of liberty, freedom and independence in their course of learning (El-Hussein and Cronje, 2010). In a reported article by Taleb and Sohrabi, (2012), students who use mobile technology devices have more motivation for learning than those who do not. Walker (2007) pointed out that the importance of mobile learning does not dependent exclusively upon the capability to use a small portable wireless device successfully. The author argued that the type of learning activity experienced by mobile owners is unique because knowledge is received and processed within the context in which the learner is located. The context is completely individual and totally different from the rigid configuration of the conventional classroom, lecture room, or science or computer laboratories.

Recently, mobile learning is one of the developing areas in the teaching and learning sector as it is getting more accepted, popular and widespread (Traxler, and Koole, 2014), which is possible with the improved accessibility and major enhancement in the capabilities of mobile devices in terms of processing speed, screen sizes, memory capacity, storage volume and network connectivity. In addition, the use of these modern mobile devices is in line with the planned ‘international educational goal’ to improve students’ learning absorption and retention, support separation of learning requirements, and reach out to students who would not use their devices to participate in learning activities (Kukulska- Hulme *et al.*, 2009).

Wu *et al.* (2012) showed that mobile learning is most commonly used by university and higher education learners, followed by primary school students, and then adult or life-long learners and lastly secondary school students. Their research further indicated that m-learning is mainly used by students in HEIs studying applied sciences, followed by the humanities, and then formal sciences, and then social sciences and lastly natural sciences. Research studies have identified three techniques for integrating m-learning devices with the mainstream of pedagogical instrument. The m-learning device can be a supportive tool, an instructional tool, and an assessment tool. As a supportive tool, a mobile device can be used to support

communication between learners and their instructor, as a file sharing mechanism, discussion medium, as well as information search device. As an instructional tool, a mobile device can be used by instructors to give learners e-books, content, and other learning materials. Also learners, for example, can execute their learning tasks on mobile devices (Gikas and Grant, 2013). Furthermore, a m-learning device can be used to evaluate students' learning activities as an online quiz or assessment tool (Ozdamli, 2011).

Many recent research studies have focused their work on the effectiveness of mobile learning and majority of their outcome showed positive effectiveness. An observation study by Evans (2008) on the effectiveness of mobile learning in a university setting showed that students prefer podcasts to their textbooks as a learning aid. Furthermore, McCarty and Carter (2013) investigated learners' performance in microeconomics courses and they discovered that the average final grades in the online classes were slightly higher than the average grades for the face-to-face classes. The effectiveness of m-learning based on the perceptions of higher education learners found out that m-learning improves retention among university students. Web 2.0 also has a positive effect on m-learning as **Terras and Ramsay, (2012, pp.6)** indicated that "By its very nature, not only can Web 2.0 generally support education but mobile Web 2.0 in particular also has the potential to blur the boundaries between formal (planned, scheduled, structured, facilitated and class based) and informal learning environments (opportunistic, non-facilitated, non-class based and entirely learner driven) and become an integral part of the process of learning and teaching".

However, the effectiveness of m-learning faces some constraints. Vogel *et al.* (2009) listed the constraints in three dimensions which are the human dimension (students and instructors), the design dimension (content and technologies), and the institutional dimension (universities, colleges and schools). The human dimension includes distractions, noise, differing comfort levels, and differing visibility levels. The design dimension includes small screen size, inadequate memory, short battery

life, inadequate built-in functions and the complexity of adding applications. The institutional dimension includes network speed and connectivity, content and software application limitations.

A lot of research in m-learning has pointed out that it can neither replace nor displace classroom or other learning approaches, but can only complement and add value to the existing learning methods (Ozuorcun and Tabak, 2012), therefore efforts should be directed at integrating m-learning with other learning methods. The integration of m-learning with classroom and e-learning is considered as a form of blended learning strategy. Blended learning as described by Picciano et al. (2013) combines the strength of classroom face-to face with technology enhanced e-learning or m-learning to maximize the benefits of both face-to-face and online methods of education.

2.2.3 M-learning Devices

Mobile learning focuses on mobility and learning through interaction with personal mobile devices. Although mobile devices were initially developed and primarily used as communication equipment like fixed wired telephones, researchers and telecommunication experts have been exploring ways of deploying mobile devices in learning and education (Berge and Muilenburg, 2013). A mobile device is a small computing appliance designed for many purposes, which include phoning, SMS, mobile internet, gaming, photography, data transfer, navigation and multimedia. These devices offer users the functionality and convenience of computing while on the move. Mobile devices are also known as handhelds, handheld devices, handheld computers, or pocket-size devices, weighing less than one kilogram. They usually come with a touch or non-touch screen interface and sometimes, with a miniature keyboard and mouse (Berge and Muilenburg, 2013).

The common mobile devices used for learning are mobile phones, smartphones, personal digital assistants (PDAs), tablets, e-book readers, net books and notebooks.

Mobile devices also include specialist portable technologies used in science labs, computer labs, and engineering workshops, environmental or geological study and in agriculture and farms. The research by Wu et al. (2012) indicated that the use of mobile phones, smartphones and PDAs in m-learning, mostly in higher education institutions, has expanded significantly from 2010, and presently, they are the frequently used mobile devices in m-learning and research, but new ones are emerging as technology improves. Similarly, tablets and net books are among the favourite mobile devices which offer all the conveniences of a personal computer (PC). The numbers of mobile device are increasing, serving as alternatives to PCs. Not only the number of devices, but the use of them, is also growing. While some of the examples of common mobile devices given above are large appliances and cannot be easily carried about, many researchers are of the view that mobile devices in the context of mobile learning should be limited to education and training on devices that individuals can comfortably carry around in hand or pocket (Behera, 2013).

Mobile devices generally have the capacity to be connected to the internet most of the time in order to be fully functional to deliver content and instruction to learners. Connectivity can be enabled either through wireless networks or mobile device networks or both. Once connected, a shared network can be created by connecting the mobile devices to data collection servers, other devices or to a common network linking to institutional systems in a way that supports a portable, digital and wireless mode of teaching and learning. Mobile devices can be connected to the internet by using a variety of different wireless communications technologies or protocols such as Wireless Application Protocol (WAP), Wi-Fi, Bluetooth, General Packet Radio Service (GPRS), and third and fourth generation (3G/4G), they can as well be connected among themselves using Bluetooth (Berge and Muilenburg, 2013). Most common m-learning devices such as smartphones and tablets connect to the internet via Wi-Fi, 3G or 4G mobile internet connections. If there is wireless technology within the institution environment or household, the mobile device could be connected to the internet or learning servers through Wi-Fi technology. There are

public Wi-Fi hotspots which can also be connected to for internet browsing. However, if there is no Wi-Fi connection, 3G or 4G connection services provided as mobile broadband to portable devices can step into the breach.

2.2.4 Relationship between e-learning and m-learning

Researchers have pointed out that the new learning technologies can neither replace nor displace classrooms completely, they can only complement and add value to existing learning methods (Ozuorcun and Tabak, 2012). Similarly, both e-learning and m-learning can neither replace nor displace each other; however, efforts are being directed at integrating m-learning with e-learning and with other learning methods. The integration of m-learning with classroom and e-learning is considered as blended learning (Picciano et al., 2013). M-learning is being considered as an integral part and a derivation from e-learning as some scholars have observed that m-learning is a mere extension of e-learning and they see no reason for adoption of m-learning into their teaching curriculum (Ozuorcun and Tabak, 2012). They based their argument on the fact that m-learning and e-learning are closely related and share many similarities. While the two learning platforms have many things in common such as self-paced and flexibility, it can, however, be argued that m-learning is not a mere extension of e-learning, but rather a different learning paradigm and approach to modernise learning activities. Table 1 below shows some distinctions between e-learning and m-learning platforms. While e-learning has taken learning away from classrooms, m-learning is taking learning to anywhere and anytime, a form of ‘learn as you go’.

Similarly, e-learning is an alternative to classroom learning; m-learning is a complementary activity to both e-learning and traditional learning. Whilst e-learning platforms offer the conveniences of personal computers (PCs), desktops or even laptop machines and net books for learning purposes, tablets and smartphones are among the favourite mobile devices used in m-learning. It is worth noting that the numbers and usage of these mobile devices are also increasing, allowing them to

serve as alternatives to PCs, most especially among students. The differences between e-learning and m-learning are also prominent in the entire different paths that are used in information presentation, instructional design, graphics and user experience design (Kambourakis, 2013)

Table 2.1: A comparison of e-learning and m-learning

| | e-learning | m-learning |
|----------------------------|--|---|
| Devices | PCs, laptops, netbooks | Tablets, smartphones, mobile phones |
| Mobility | Private location | Anyway, anytime |
| Materials and instructions | Online notes, URL links and slides. Can be downloaded. | URL links. Can be downloaded. |
| Presentation | Usually formal and structured | Usually informal and situated |
| Communication | Whiteboards, chat rooms, discussion boards, emails | Instant messaging, alerts, SMS, emails access to whiteboards and discussion boards. |
| Connectivity | Wired or wireless (Wi-Fi) | Multiple wireless interface e.g. Wi-Fi, Mobile Network |
| Assignments | E-mail attachment or web posting | Web posting, app access |
| Assessment | Online exams, feedback through email | Feedback through email |

Furthermore, e-learning is generally presented in a formal and structured way, in contrast, mobile learning is often adapted for informal learning, that is, is it being used for learning in a more relaxed and comfortable environment.

Considering the rapid development in mobile technology, it is essential for any e-learning system to fully support portable devices so that learners can effectively conduct their e-learning activities via their mobile devices. With the integration of

mobile devices as well as the interactive involvement of their users, e-learning systems could become a kind of universal mobile computing platform for all distance learning students.

2.3 Overview of Security Issues in E-learning and M-learning

There are concerns that have evolved from the use of modern technologies for learning that may affect their adoption negatively, the important ones being the security risks and vulnerability attack issues on learning contents and private information on m-learning devices (Kambourakis, 2013). The security issues inherent in these devices are also applicable when they are being used for learning. There are perceived security risks, as such students interfering with learning content and instruction as well as other real risks. Securing the e-learning and m-learning environment requires avoiding and preventing four types of threat, which are fabrication, modification, interruption and interception of learning content or instruction, and safeguarding confidentiality, integrity and privacy, as well as protecting against manipulation and piracy (Mulliner, 2006). Access control is important in order to avoid all these threats on ubiquitous learning platforms and one of the ways to do this is via the use of authentication and authorisation processes.

Security issues in learning platforms that have been exploited are related to vulnerabilities in the operating system and flaws in the application software or network facilities (Jang-Jaccard and Nepal, 2014). Most e-learning and m-learning applications are built on three-tier architecture, comprising a database tier, an application tier, and a client tier. Many security issues in e-learning are also applicable to m-learning due to the similarities in their architectures. Most security issues that are common to both learning systems occur at the database and application server levels, while there are few dissimilar security issues at the client level.

2.3.1 Security issues common to e-learning and m-learning systems (Database and Application Server levels)

- **Cross Site Scripting (XSS)** is one of the most common application-layer security issues attacking the web-pages. XSS is a threat emanating from internet security weaknesses of scripting languages, with HTML and JavaScript as the prime culprits for this exploitation. XSS normally targets scripts embedded in a page which are executed on the client server-side. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user. Such a manipulation can embed a script in a page which can be executed every time the page is loaded, or whenever an associated event is performed. An XSS attack can be used to achieve the following malicious results: access sensitive information, identity theft and alter browser functionality. However, XSS threats can be reduced by safely validating untrusted HTML input, setting up cookie security on browser, using content security policy, implementing JavaScript sandbox tools and using various auto escaping methods (Hydara et al. 2015).
- **Cross Site Request Forgery (CSRF)** is an attack that tricks the user into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired manipulation function on their behalf, like change the student's record such as e-mail address, home address, password or even grade. CSRF attacks generally target functions that cause a state change on the server but can also be used to access sensitive data (Luminita and Magdalena, 2012). For most sites, browsers will automatically include with such requests any credentials associated with the site, such as the user's session cookie, basic authentication credentials, IP address, Windows domain credentials, etc. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish this from a legitimate user request. CSRF prevention techniques

work by embedding additional authentication data into requests that allow the web application to detect requests from unauthorised locations.

- **SQL Code Injection** in the site address performs different searches using search engines to retrieve personalised web-site information like password and username cracking using decryption tools. Using this method, a hacker can pass string input to an application with the hope of gaining unauthorized access to a database. Hackers enter SQL queries or characters into the web application to execute an unexpected action that can act in a malicious way. Such queries may access unauthorised data, bypass authentication or shutdown a database even if the database resides on the web server or on a separate server. SQL injection can be applied also to URLs, which can be modified by an attacker in order to access important information. SQL injection can be avoided with strict adherence to some basic security practices. Some of the methods to prevent this kind of SQL injection vulnerability are: checking the user's input for dangerous characters like single-quotes; using prepared statements, which tell the database exactly what to expect before any user-provided data is passed to it; encrypt sensitive data; ensuring that error messages give nothing away about the internal architecture of the application or the database.
- **Stack-smashing attacks** is a type of buffer overflow attack that targets a specific programming fault such as inappropriate use of data buffers allocated on the program's run-time stack, local variables and function arguments. A stack-smashing attack is a serious problem, since an innocuous service (such as a web server or FTP server) can be made to execute arbitrary commands. The idea is pretty straight forward: insert some attack codes (for example, code that invokes a shell) somewhere and overwrite the stack in such a way that control gets passed to the attack code (Peltier, 2013). It can be avoided by using a language or compiler that performs automatic bounds checking and using technologies that attempt to protect programs against these attacks.

- **Session Hijacking** is the exploitation of a valid computer session, sometimes called a session key, to gain unauthorised access to information or services. Session Hijack achieved by giving a unique session id to the browser, either in a form of cookie or URL, which the browser submits with every new request. The session is active as long as the browser keeps sending the session id with every new request. The attack is possible when the session id is weakly encrypted, too short or assigned sequentially. Sessions that do not expire on the HTTP server can allow an attacker unlimited time to guess or brute-force a valid authenticated session id and eventually gain access to that user's web accounts. Additionally, a session id can be potentially logged and cached in proxy servers. When transmitted via a URL parameter, requests can potentially be stored in the browser history, cache and bookmarks. It can also be easily viewable afterwards. One method to prevent session hijacking is to set a secure session link via HTTPS (Peltier, 2013).
- **Denial-of-Service attacks (DoS)** attacks render a service or device unusable for its legitimate use by denying availability. A successful attack will shut down or dramatically limit the operation time of the target, thereby depriving the users of the services of a resource what they would normally expect to have. It is aimed at complete disruption of routing information which consequently affects the whole operation of the wireless network and normally affects the availability of a computer system. Such attacks could exploit different functionalities, like CPU intensive tasks that require a lot of energy. DoS attacks can be avoided using prevention techniques for counteracting DoS such as protocol traceback techniques on the servers (Tupakula and Varadharajan, 2013) and reverse proxies spread across multiple hosting locations.

It should be noted that these security issues are general ones that are not specific to e-learning and m-learning applications and database systems. They are normally found in any three level system. Just as learning systems are production systems to

educational institutions, security becomes a fundamental requirement. As ubiquitous learning platforms increase in demand and popularity, the need to improve their security also increases and inevitable (Zafar *et al.*, 2014)

2.3.2 Security issues in e-learning and m-learning (Client level)

The client level of e-learning and m-learning are prone to digital and physical attack and threats. Malware, viruses, spoofing, loss/theft and unauthorised access are some of the security issues at client level. Given their high portability, mobile learning devices such as smartphones and tablets are more susceptible to physical and digital attacks than desktop and laptops that are mainly used in e-learning. Digital attacks are common in mobile devices mainly due to vulnerabilities that remain in the development process of mobile software or services. Furthermore, while PCs and laptops have some inbuilt security software such as firewalls and antivirus software, mobile devices generally do not come with protective software.

According to Mulliner (2006), mobile device security has five main basis that distinguish it from conventional computer security: (i) mobility, (ii) strong personalisation, (iii) strong connectivity, (iv) technology convergence, and (v) reduced capabilities. Mobile devices are portable and movable, so they are not kept in one place which may be secured, and therefore, they might easily get stolen and physically tampered with. Strong personalisation implies that mobile devices are normally not shared between multiple users, while desktop computers are often shared. Strong connectivity gives mobile devices support for multiple ways to connect to a network or the Internet. Technology convergence indicates that mobile devices can combine or have many different technologies in one device. Reduced capabilities mean that mobile devices are computers but lack many features that desktop computers have. For example, a mobile device does not have a full keyboard and has limited processing capabilities.

Considering the facts mentioned above, it can be observed that mobile device security is more complex to deal with than a normal PC. Each additional feature in a mobile device adds at least one new target that can be attacked or an additional security risk. For example, mobility increases the risk of theft, because stealing a mobile device is a lot easier than breaking into a PC. In fact, one survey found that one out of every three users has lost their mobile device at some point in time (Juniper, 2011). The strong personalisation and connectivity increase the threat of identity risk and privacy violations because a mobile device is always with the owner and locating the device means locating the owner. Reduced hardware capabilities may facilitate certain kinds of denial-of-service attacks. Furthermore, some missing features, such as lack of an external keyboard may complicate the use of effective authentication mechanisms (e.g. username and password). All these features bear further implications, like increased complexity when conducting security audits of mobile devices. Table 2 below summarises the security issues in both e-learning and m-learning client level.

However, some manufacturers of tablets and other mobile devices are now giving security consideration in the design of their devices and apps installations. For example, Apple's restricted access platform design and rigorous applications screening procedures greatly reduce the risk of downloading malicious software from apple store. Furthermore, as Apple does not provide built-in anti-virus software, third-party anti-virus apps are restricted from accessing the necessary layers on iPads or iPhones to provide effective anti-virus security and currently there are no effective anti-virus software solutions available for iPads and iPhones.

Table 2.2: Security issues in e-learning and m-learning (Client level)

| | e-learning clients | m-learning clients |
|---------|---|--|
| Devices | Less prone to physical attack and theft. Can be secured by lock/key or security cable | More prone to theft and loss. Can be tracked using GPS app |

| | | |
|------------------------------|---|--|
| Software | Have inbuilt security software such as anti-virus and firewall | Does not usually come with security app. However, security app may be purchased or downloaded for free |
| Capacity | Have good hardware and software capabilities to withstand security threats such DoS | Reduced capabilities and missing features facilitates certain kind of attacks. |
| Mobility and Personalisation | Less mobility and personalisation in desktops and PCs. Less mobility | Strong personalisation and mobility increases identity risk and privacy violations |

However, mobile devices having Android and Window operating systems have online security vendors from whom security apps can be purchased or download for free. For example, Norton Mobile Security is available for Android tablets and smartphones. Windows tablets come with Microsoft free security software such as Windows Defender. Both e-learning and m-learning client level devices are prone to physical attack and theft. M-learning devices, however, are more susceptible to attack. E-learning client devices such as PCs and laptops may be locked away or secured with a laptop security cable which is one of the easiest methods of protecting laptops against theft, m-learning devices may only be tracked after theft using a GPS app, provided it has been previously installed and is running.

Having covered the overview of security concerns in e-learning and mobile learning systems, it is important to review scholarly publications on the topic. Some researcher scholars, such as Zamzuri *et al.* (2013), observe that students, being one of the stakeholders in the educational sector, use their mobile devices for learning and they are worried about their privacy and security when accessing m-learning system. The authors indicate that students are concerned that their confidential information such as their assessment grades, personal details and examination feedback might be exposed to their colleagues, thus the authors propose that students' needs and views should be

given adequate consideration during implementation. Alwi and Ip-Shing (2009) observed students' perceptions of an e-learning system (mobile learning is a subset of e-learning) and revealed that there are security concerns in the e-learning system by the students, and the authors concluded that reliability in an e-learning system is important in securing patronage for the modern learning environment. While these two studies highlight confidentiality and privacy as issues, they are more peculiar to an e-learning environment, and they did not discuss in detail these security issues and failed to mention other threats that users may encounter when using their mobile devices for learning purposes.

Hasan *et al.* (2014) agree that security is an important aspect of open, interactive and distributed learning systems like e-learning or m-learning and that considerable effort should be put into development of the content and infrastructure for online systems to avoid attacks and ensure the reliability of technology to users. Tugui *et al.* (2008) discuss the components of an e-learning platform that are susceptible to attack, and possible vulnerabilities that may affect the security of the online teaching and learning system, such as DDoS and key-loggers which may be installed by students to steal lecturers' passwords and modify grades without permission.

Levy *et al.* (2013) conducted a study to assess the severity of security attacks on an e-learning platform to find out the ethical implication of the attacks. The five types of security attacks investigated in their study are: (i) attacks on the server, (ii) e-mail interception, (iii) unauthorized file sharing, (iv) unauthorized access, and (v) spoofing attacks. The outcome of their study shows that 90% of the participants viewed these attacks as unethical while 3.24% of the participants indicated that the cyber-security attacks are ethical. While these studies considered the security attacks on an e-learning system, the results are applicable to mobile learning to a large extent as mobile learning is a subset and/ or extension of e-learning.

2.4 M-learning Security Issues in Nigerian HEIs

The concern about security risks and privacy issues in the m-learning realm seems to be quite high in the Nigerian HEI environment and sadly, there has been little research on m-learning and related issues within the Nigerian HEI context (Osang *et al.*, 2013). There are limited m-learning security journal papers to raise necessary awareness among stakeholders, particularly among the students. This section reviews and evaluates the current literature on m-learning within the country's HEI's and gives insight into security and privacy matters.

In Nigeria HE context, Chaka and Govender (2017) indicated that m-learning is providing access to education for many students and it is playing a vital role in bringing education to students living in rural and remote communities especially in nomadic environment. Another study on m-learning in Nigeria by Rafiu *et al.* (2011) emphasized that learners are well prepared and ready for mobile learning as they have various types of mobile devices in their possession and demonstrated high level usage skills for successful implementation of mobile learning. Adedaja *et al.* (2012) stated that m-learning allows students to send and receive learning content that contains graphs, images, video and sounds, making it a platform to create reality and dynamism needed for effective learning. They remark that mobile technologies improve the productivity and efficiency of learners in Nigeria by delivering educational materials and support in real time and in the right context for their immediate needs, and they conclude that having a good mobile technology infrastructure in the absence of other alternatives has made m-learning a good choice for Nigerian students. Although the authors discussed the importance of m-learning to the Nigerian educational system, they did not give any insight into the shortcomings of such a ubiquitous learning system within Nigeria HEI context.

Okeke and Umoru (2012) discussed possibilities and challenges of m-learning in Nigerian universities. The challenges the authors raised on m-learning devices include small screens, tiny keyboards preventing efficient input, high prices, and limited computing capability and connectivity issues. They further mentioned the lack of technical experts in the mobile learning field, and adaptation of mobile software for the Nigerian educational curriculum, as some of the challenges facing m-learning in higher education institutions in Nigeria. **While their research is a significant piece of work on mobile learning in Nigerian HEIs, they failed to address security threats as a challenge in Nigerian universities. Furthermore, the latest mobile devices have screens that are big enough and keyboards that are suitable for learning, even the newest mobile devices have powerful computing capability while their prices are also falling significantly (Kagan, 2014).**

In a recent study conducted by Osang *et al.* (2013), 56 out of 80 educators (representing 70.1%) interviewed considered security issues as one of the main barriers to successful implementation of mobile learning in Nigeria. They stated that educational institutions, educators, and learners are extremely concerned about the growing threats to data security and privacy. The authors argued that if lecturers want to go by the security challenge currently facing the country, the lecturers will prefer their identities to remain confidential as a preventive measure towards falling target to unsuspecting mischief makers who can use their identity to perpetrate malicious acts. The authors identified the adverse effects of social media on mobile learning which include joining negative groups on social media by the students, which may threaten their personal safety and the security of their handheld devices. The authors further highlighted the potential dangers unassuming people are exposed to in the hands of those who misuse mobile technology. **This work is relevant to Nigeria HEIs because it discusses the prospects and challenges of mobile learning in Nigeria and their study was carried out in the same geographical location, however, it failed to mention specific security challenges the educators are facing when using mobile devices as teaching aids.**

2.5 M-learning in an alternative education environment

Alternative education is a form of all educational activities outside the traditional main stream school system that addresses the needs of students that typically cannot be met in a regular school. It relies on the perception that there are many ways to be educated and there are many types of environments or structures in which educational activities may takes place. Thus, alternative education recognises that everyone can be educated and to accomplish this, alternative education provides a variety of ways or avenues such that individual can find a suitable or comfortable one to facilitate learning process (Kraftl, 2013).

Integrating m-learning into alternative education will further promote its objective that education may occur in many kinds of environment and locations. Apart from this, incorporating m-learning in alternative education has many other benefits. Firstly, alternative education programs are often viewed as opportunities designed to meet the educational needs for individualized identified as at risk for academic failure, integrating m-learning will make the students learn on their own time and space, which may invariably reduce failure. Secondly, students with emotional or behavioural disorders are often enrolled in alternative education settings due to behaviour that cannot be supported in a mainstream education, having alternative education programs on mobile devices may be an effective intervention for the students to make appropriate behavioural changes by privately engaging with the devices rather than displaying behaviour among themselves (Flower et al. 2011).

Thirdly, alternative education recognises that all students do not learn in the same way, therefore they should not be taught in the same way using a common curriculum. It accepts that all schools do not have to be same or pose similar learning settings. Consequently, using m-learning in alternative education

implies incorporating many choices within school to ensure that all students may find a path to their learning objectives. Lastly, alternative education enables students within the same school to pursue common goals through varying approaches, which may include ubiquitous learning platforms such as e-learning and m-learning (Kraftl, 2013). Therefore, integrating m-learning into alternative education will make learning more flexible with increased personalisation as it does in mainstream schools. Similarly, the m-learning security issues that students in alternative education may experience is likely to be same with those experiences in mainstream education. Further studies, however, may be needed to support this assertion.

2.6 Education in a Wider Context

Aside the description and use of education as knowledge delivery, education is applicable to formal and informal environments in relation to m-learning that occurs in many places, such as home, community, religious grounds and work places through interactions and collective relationships among various members of the community or organisation. Thus, in the home and community settings, education may be used for language acquisition, cultural norms and manners acceptable within the community. In a religious environment, education can be used for teaching and learning the ethics and beliefs guiding a particular religion. Therefore, education in a broad context outside knowledge delivery is largely determined by complex social practices, which consist formal and informal parts (Manuti et al., 2015).

In a formal organisation such as offices, education is being used for workplace teaching and learning programme and for training and retraining employees. Workplace learning and training can take on different forms, including e-learning education, attending conferences, making presentations and use of

mobile devices for learning among the employees. E-learning programmes are being introduced in many organizations as part of induction courses to train new employee. Recently, many organisations are integrating educational technology using e-learning platforms in their corporate networks to train their employees, make them interact with one another, extend services and circulate their policies and procedures easily and effectively among staff (Cheng et al., 2015). Manuti et al. (2015) indicate that education in a work is positively connected to flexibility, employability, interactivity and adaptability to workplace environment.

2.7 Summary

In summary, we can conclude from section 2.1 that in an educational context, mobile phones are broadly used by students to access and support learning. Thus, the main focus of m-learning is to utilise the substantial development in mobile technological advancement to the utmost advantage of the learners to improve their learning process and shorten the learning curve. Another focal point of m-learning is to facilitate information sharing, which makes it possible for learners to interact with each other and share knowledge anytime. The use of mobile technologies by learners, however, has implications for security in term of integrity, confidentiality, and privacy of the users' data who are involved in the learning process as discussed in section 2.3. In this regard, learner records, e-portfolio data, assessment grades and feedback are some examples of sensitive information that need protecting when using mobile devices in education (Kambourakis, 2013). Therefore, the challenge is to safeguard what should be learnt in the lecture room, what should be learnt outside the classroom, and the methods in which connections between these two settings should be made (Hashemi *et al.*, 2011). The security needs of any digital learning platform are to protect the content, services and the personal data of the stakeholders. Their confidentiality should be guaranteed at all times (Luminita and Magdalena, 2012).

This chapter evaluates past and current developments in the modern learning environments, in particular distance learning, e-learning platforms and mobile learning, it identifies the present positions of the pedagogical learning platforms and shows the difference between e-learning and m-learning in section 2.2. This review chapter is then narrowed down from general concept of e-learning and m-learning to the security aspects in section 2.3 by evaluating the security, privacy and trust issues in these learning platforms and making comparison between the security issues in e-learning and mobile learning systems. Section 2.4 of this thesis further identifies gaps and problems within Nigerian Higher educational institutions in terms of m-learning security by evaluating the available journals and articles in this regard. The identified security concerns in section 2.4 serve as motivation to conduct this research. The chapter concludes with the review of mobile learning in an alternative education environment.

CHAPTER III

Methodology

3.1 *Introduction*

One of the significant parts of any research is to choose a suitable methodology, which involves using appropriate tools, techniques and steps in finding solutions to the research questions. This chapter discusses the research methodology that has been used in this thesis and how it has directed data collection, design, implementation and evaluation activities. The methodological procedures upon which this study is based are used as guidelines at different stages of the research, along with different research techniques that are chosen to gather sufficient and relevant data in order to achieve the objectives of this study by providing answers to the research questions. The research methodology has been carefully formulated and developed, keeping in mind the purpose of the study and the research questions to be answered. The identified research objectives in chapter one have been considered in determining the appropriate research methodology for this study.

This research is interdisciplinary and combines theories from education and computer science. Thus, this research adopts educational models, such as student-centred learning approaches and computer science models, such as user-centred design and evaluation, Technology Acceptance Models (TAM), and the generally accepted system security principles (GASSP). Therefore, the research methodology used in this study is approached using the mixed mode methodology in which all stated models and principles are employed in order to develop accepted solutions for the stakeholders in HEIs in Nigeria, particularly the students who are the main users. As a result, our methodology has embraced a user-centred model, a student-centred, model and TAM throughout the practice of preliminary studies, app design, initial and post-study evaluation and validation. Furthermore, a user-centred methodology for design and evaluation has been considered within all the research activities

conducted in this thesis, along with other research-based methodologies which are used to investigate the design and evaluation of the proposed security enhancement solution. This mixed methodology approach is being applied at a variety of key stages of the research, including the literature review, user-centred design, iterative development and implementation and user-centred evaluation, as outlined below.

3.2 Overview of the Methodological Approaches

3.2.1 Document review

Document review which comprises literature and journal reviews in chapter two and some unpublished materials obtained from academic and management staff during the research is the backbone of this research being the first activity embarked upon at the beginning of this study. The literature review included in Chapter two was done to assess the contemporary findings in the area of study. The period of review commenced in early 2013, and continued up to the time of completion of the study in late 2016 to ensure it is always up to date. The literature review concentrates on the areas of m-learning, e-learning and the security threats within the learning platforms with regard to the security challenges in HEIs in Nigeria.

The purpose of including the document review within the methodology is to ensure that the research content is current with the available latest developments in the field of study. This will also ensure that the researcher is keeping abreast of the current events within the field and is aware of the state of the art technology in his field of study. Another reason for including the literature review in the methodology is that, being the starting point of this research, it served as a pointer to understand what has been researched and what has not in the area of m-learning security. Also, this approach has been used throughout the thesis and it has

helped in decision making on m-learning security framework development, app design, evaluation and implementation and other follow-up activities.

The documents and journals used in this research are drawn from credible academic sources such as the IEEE Xplore online library, ACM digital library, google scholar amongst many other online journal portals were used to obtain peer reviewed journals articles. Information was also collected from various publications through books, online reports from internationally recognised bodies such as UNESCO and from the archives of the participating institutions in Nigeria. Academic databases such as the Scopus database were used to identify peer-reviewed journal articles and conference proceedings.

3.2.2 User-Centred Design (UCD)

User-centred design (UCD) can be described as a multidisciplinary design approach in which the needs and limitations of end users are given attention at every stage of the design process with the aim of improving the understanding of researcher (Galer *et al.*, 2016). This user-centred design methodology is used as part of the research methodology in many research studies involving users. As this research focusses on users (students and other stakeholders in academia), the user-centred design methodology (UCD) is used throughout the research, particularly in security framework design in chapter six, specific experiments in chapters four and five, app design and implementation in chapter seven, in order to obtain users' needs, requirements and opinions on the research. Consequently, this approach has been adopted from the early stages of this research as recommended by (Mohammadi, 2015), combined with the TAM and generally accepted system security principles (GASSP) to develop the first prototype of the m-learning security framework and m-learning security enhancement app. Thus, the use of user-centred design (UCD) is considered from the initial research assessment stages so that more user-friendly systems can be built (Preece *at al.*, 2015).

The aim of using a user centre design approach methodology is to provide the users the opportunity to express their perceptions, allow them to express their feelings and concerns on what is considered appropriate for enhancing their security when using mobile devices for learning (Quintana et al., 2013). It also helps the researcher to understand what the problems users are facing or encountering regarding m-learning security. At the initial planning stage, user-centred design questionnaires and interviews, were adopted, in order to specify users' requirements. The subsequent chapters in this thesis outline the exploratory study that has been carried out using this approach, with the aim of identifying a set of requirements for an initial security enhancement framework as well as gathering data on concerns and preferences for further research. This approach was also used repeatedly at a later stage of the research in form of case studies and focus groups, when further improvement was needed on the first design.

This approach, therefore, allows gathering a pool of design needs that should be addressed in the theoretical model and app development. It facilitates the users' participation in order to achieve a good level user experience in relation to the system design, functionality, usability and users' acceptance. The benefit of using user-centred design (UCD) is to produce an appropriate methodology along with discussion points mentioned above and its connection to the research questions, in order to enable the researcher to understand m-learning security issues within the context of HEIs in Nigeria. The significance of user involvement in the design and development processes of any user-driven system or app can no longer be overlooked, because of their contribution to the effectiveness, efficiency, and usage (Quintana et al., 2013). There are, however, some drawbacks associated with the user-centred design methodology such as extra costs and slower development, which were put into consideration in the research timeframe.

Many system design standards and principles were reviewed and explored with the conclusion that, this research focusses on UCD, one of the suitable standards for this research is the ISO-standard 9241 -210 (formerly known as ISO – 13407), which is based on Human-centred design for interactive systems (Giacomin, 2014.), this standard presents a high level overview of the activities that are recommended for human centred design for mobile phones. The standard describes six key principles to ensure that the design is user centred, which needs to be carried out, starting from the earliest point of the research.

- **The design is based upon an explicit understanding of users, tasks and environments.**

This principle ensures understanding the users within the 'context of use'. This principle was adopted in this research by applying the ISO-standard 9241 - 210 process on need to understand the users, understand what they want to do with the system and also understand the environment in which the system is used (Travis, 2011). This was implemented during the early stages of the research, as presented in Chapters five and six.

- **Users are involved throughout design and development.**

The purpose of this principle is to ensure that the designer involves users in all design phases take active parts in development. This is implemented in this project engaging users in design stages, their input and recommendations are valued and incorporated to make a better release. It is also achieved through field studies carried out during the design and usability evaluation activities.

- **The design is driven and refined by user-centred evaluation.**

To ensure that the users are an integral part of every stage of the process, there are some empirical methods that can be used. Interviews and questionnaires are highly appropriate for creating user driven design solutions. These methods are employed, as they are proven to be the most suitable means of obtaining information (Page, 2011). They were chosen as the most cost-effective methods of gathering data for the research in this thesis and were used to collect information and identify needs. The standard points out that usability evaluation should be carried out throughout the design process. The description of the way the questionnaires and interviews are applied in practice is provided in Chapters four to eight.

- **The process is iterative.**

The standard simply states that most appropriate design for an interactive system cannot typically be achieved without iteration. This is part of the experience gathered during this research as the first app developed, though was good at improving user security in m-learning, it was not adequate enough and was later improved upon, and the research eventually developed a final app describe in chapter seven.

- **The design addresses the whole user experience.**

The fifth stage involves evaluating user experience of the system by including the kind of perceptual and emotional aspects typically associated with user experience. This method involves monitoring users' behaviour on the system and gathering information on their usage (Travis, 2011). The implementation tool used in the research for this purpose is app logging activity along with users' responses during the interview stages. The feedback which has been evaluated appropriately as detailed in Chapters five to eight.

- **The design team includes multidisciplinary skills and perspectives.**

The final point of standards is including a range of views in the system such as the voices of experts, users, domain experts, marketing, technical supports and writers and business analysts. It is to ensure that a robust solution is achieved and delivered at the end of the project. The relevant people involved in this research include students, academic staff, experts from the computer security field and university non-teaching and administrative staff who are involved in m-learning and security, the experience of these stakeholders are discussed in Chapter four.

3.2.3 Iterative Development and Implementation

This study is conducted using the iterative and incremental development model which is a form of cyclic system development process. With this model, the security enhancement app undergoes repeated cycles during the development stages, making sure that technological modifications to the initial specification are met through the use of iterative processes following a clear set of objectives which are contained within each iteration set. The refined app which was achieved through a series of iterations, extends upon the previous iteration while each iteration entails evaluation, implementation, design and other development processes. Each prototype improves on the previous version by fixing the weak points or adding new features. This approach allows tracking the maintainability of the initial app design and the final version. The final app is a product of an evaluation method for the user-centred design and technology acceptance model. For this research, the m-learning security enhancement app has gone through two main iterations for features improvement. Further descriptions on the iterative system implementation applied in this thesis are discussed in Chapter seven.

3.2.4 User-centred Evaluation

For the purpose of evaluation, the User-centred Evaluation (UCE) model was employed as a guideline for conducting evaluation experiments along with the technology acceptance model TAM, as a methodological approach of evaluation of the experiments and case studies conducted in this research. The User-centred Evaluation (UCE) analyses the attitude of the users and their perception on the quality of the application. Although perceptions might be subjective, this approach is an effective means of appraising and evaluating experimental systems and applications (Van Velsen *et al.*, 2008). Thus, the User-centred evaluations in this research focus on effectiveness and efficiency of the application, as these features can be used to evaluate which specific components of the system played a major role in attaining users' expectations or acceptance.

User-centred Evaluation is used in this research because it is considered as one of the commonly and well-accepted approaches in evaluating user experiences or opinions on the quality of the service provided by an application (Quintana et al., 2013). This is because User-centred Evaluation functions well and fits in perfectly when used for evaluating experimental systems and applications. Secondly, the UCE methodological approach sets the evaluation conditions and guidelines for both the facilitator and the users when conducting the experiment. Thus, UCE can be used in any application domain, as long as the evaluation measures that are connected to the domain are justified. Thirdly, in this research, the users have been the key focus in both design and evaluation. The users who are students and academic staff from HEIs in Nigeria have participated in the preliminary study of the research using the user-centred methodology. The users have also experimented with the application, participated in the final version design and evaluated the updated version based on User-centred Evaluation.

In order to measure the usability and acceptance of the app developed using a UCD approach, **the Technology Acceptance Model (TAM) is adopted. TAM, which is one of the successful platforms in measuring information technology acceptance and usage, focuses on two main factors: the perceived ease of use and perceived usefulness (Marangunić, and Granić, 2015). The usability and usefulness of TAM concept were examined in the early stage of this study as discussed in chapter seven. Perceived usefulness is the degree to which users accepts that using the system will change their performance in a positive way. Perceived ease of use is the degree to which users accept that using a certain system would be free from effort (Wallace and Sheetz, 2014). It is also suggested that these two factors have a significant implication on the users' perceptions towards accepting the system, and that usefulness is the most important predictor of acceptance of the technology (Ooi and Tan, 2016). The evaluation of the security framework and security enhancement app using UCE in chapter seven was carried out in line with Technology Acceptance Model.**

3.3 Data collection methods

A number of experiments and surveys were conducted to collect users' experience on the proposed research on m-learning security issues and their perceptions on the interventions. **Computer Science students** and academic staff were asked to work with the app as case studies. During the experiments, log files were stored and user activities were logged to track the users' behaviour on the system. The log files and the evaluation feedback were used for evaluating the app. At the conclusion of the experiment, participants were asked to complete a questionnaire provided along with the app so as to give feedback on the system and their overall experience. In addition, qualitative feedback was collected from academic staff who are experts in computer security, as part of overall feedback from users who were interested in giving further

suggestions. Details on data collection methods and justifications are described in the relevant chapters.

3.3.1 Quantitative

In this research, quantitative methods are used as strategies for data collection, which are normally accomplished by statistical methods to analyse findings. Questionnaire is a common approach which is used for obtaining quantitative data in a planned setup from participants (Smith 2015) and it is used in this thesis. Three types of questionnaire formats that are used when developing a questionnaire are: (i) structured, (ii) semi-structured and (iii) unstructured. Most of the time, the choice of the format is normally based on many factors, among them is the sample size. Cohen *et al.* (2013) indicated that the more the sample size of the participants, the more structured the questions may become and as the research sample size was quite moderate in all data collections, semi-structured questionnaires were used as one of the instruments to collect data in order to obtain balanced unbiased responses from the participants.

The benefit of using questionnaires is that it gives respondents the opportunity to state their opinions freely without any fear as their responses were unmonitored. Another advantage is that questionnaires can reach a large number of respondents effectively within a short time, thus it increases the response rate significantly. However, a disadvantage of questionnaires is that misinterpretation of questions may lead to inappropriate or irrelevant answers. In order to avoid this kind of problem, the researcher was available during the questionnaire session to attend to any queries that the respondents may have had in relation to the questionnaires.

Lastly, questionnaires may also be helpful in survey that involves a large number of respondents because they are likely to be more cost effective than other means. Before the distribution of the questionnaires to the participants, pilot tests are done with a small group of colleagues and the opinions and suggestions given by them

were taken into consideration in making the final copy of the questionnaires. A pilot test was conducted for the second time with another small group of colleagues in order to ensure high reliability and understanding of the questions.

Two sets of quantitative methods were administered during the research study, the first for the preliminary survey in order to gather users' experience on the security issues in m-learning, the second was presented as an evaluation of the mobile learning security enhancement app. While the questionnaires were designed based on user-centred methodology approach, a Likert scale and System Usability Scale were used in the development of survey questions, as response options for the closed questions. The designs of the questionnaires are discussed fully in related chapters of this thesis.

3.3.2 Qualitative

Along with the quantitative method, qualitative data collection through interviewing was employed. Some semi structured interviews were used to obtain responses from academic staff as indicated in relevant chapters. The rationale for using semi-structured interviews was that, they most of the time, provide a relaxed interview environment which enables positive interaction among the participants while allowing the researcher to collect rich quality data as well as preserving a semi-structured interview rule. Another reason is that semi-structured interviews provide a flexible and conducive environment for participants unlike formal interviews which have a reduced flexibility and may sometime change the interview process into a formal one in which participants may feel that they are being pressured for responses (Taylor *et al.*, 2015). As with the quantitative data collection, pilot mock interviews were conducted with colleagues and their opinions and suggestions were taken into consideration in making the final interview questions. Three sets of interviews were administered during the research study, the first for the preliminary survey in order to gather opinion on the security issues in m-learning, the second was presented to

understand if the findings are adequate and the last quantitative survey was an evaluation of the m-learning security framework and enhancement app. Details on the interviews are discussed in relevant chapters of this thesis.

The data analysis method employed in this research follows a thematic analysis approach which is based on examining themes within the data collected (Bryman, 2012). Initially, all the primary data collected through interviews and questionnaires were transcribed from a tape recorder before coding. A Pattern coding is a way of grouping summaries into a smaller number of sets, themes, or constructs, and coding pattern may be characterised by (i) similarity (that is things happen the same way), (ii) difference (that is things happen in predictably different ways) and (iii) frequency (that is how often or seldom things happen) and basically a set of structured data is an outcome of coding.

Nvivo qualitative analysis software package was used for coding the content analysis. In Nvivo coding refers to coding with a word or short phrase from the actual language found in the qualitative data record. After the raw data or notes taken by the researcher is entered into the word processing component of the program, the package assists the researcher in content identifying terms, phrases, or themes that appear in the text document. The extraction involves keyword search within the raw data in the software and then counting how many times they appear and in what context. This makes it easier for the researcher to convert the coded findings to standard statistical analysis to determine frequencies and correlations with the data and to make necessary reports thereafter in each section of this thesis.

3.3.3 Case Study

This research also makes use of case studies to collect empirical data necessary to gather valuable feedback on the findings. While Cohen *et al.* (2011) termed case

study as a challenging method, Yin (2015) considered case study as an effective method of using different procedures to correlate an argument that is relevant to the way of investigating activities that happen in a specific context. In this research, the case study involved participants using the security enhancement application during the evaluation stage and observing the activities being carried out in the process. The aim of the case study is to enable the participants to contribute to the development of the m-learning security enhancement app providing personal opinion on it. Through interviews and questionnaires on the case study, learners also provided responses based on their perspectives on how the application improves their security understanding of m-learning devices. It is important to evaluate users' satisfaction when using applications, especially in relation to their needs, therefore the case study, forms part of the user-centred evaluation methodological approach in the thesis.

3.3.4 Mixed method and triangulation

The user-centred methodology used in this research involves many field work activities carried out in university environments. Therefore, different data collection strategies were used to gather data and using more than one research method for data collection to achieve the research objectives is known as a Mixed Method. The mixed method of data collection used in this thesis employs both qualitative and quantitative methods described above as they are regarded as highly complementing rather than mutually exclusive to one another (Creswell and Clark, 2011). The mixed method of data collection allows the researcher to engage in a “triangulation approach” which involves using different methods of data collection, varying data sources, different analyses or theories to check the accuracy and validity of the findings (Lesser, 2016). The benefit of triangulation is that data obtained from multiple methods reduces the effects of limitations any one particular method may have on the data. The mixed method strategy research technique according to Bryman (2012), though it may be time consuming, it is chosen in this research to provide a balanced view of the research outcome.

3.4 Sample and sampling technique

The sampling method used in this research is a stratified sampling technique involving two processes (Palinkas *et al.*, 2015). The first process is to determine and identify the university staff and students who are aware of, and are knowledgeable on mobile learning and security. The process, therefore, involves inviting academics from Computer Science and Information Technology departments and students mostly in their year final or postgraduates in computer related courses, who have been taught some modules in computer security and mobile devices, to participate in the study. The second process uses a simple random sampling to give each member of this group an equal opportunity of being selected in order to produce unbiased results (Saunders *et al.*, 2012). The research survey comprises of students and staff of four tertiary institutions in Nigeria namely; the University of Lagos (UNILAG), National Open University of Nigeria (NOUN), Lagos State University (LASU), Yaba College of technology, Lagos discussed in section 1.6 in chapter one of this thesis.

Given that the methodological approaches used within the thesis are user-focused, it is important to select appropriate sample sizes in order to reflect the views of the actual population appropriately. The common determinants of sample size are aim of the study, the population size and the sampling error (Israel, 1992). Other factors include the level of confidence and the degree of variability attributes. Within this research, sample size has been given due consideration with all necessary factors considered. The population of students and staff in Nigerian universities was approximately 1,700,000 as at the beginning of this study in 2013 (WENR, 2013). **However, the population size of this study was computer science and information technology students and tutors in HEIs, the data was not available on the NUC website and it was not feasible for the researcher to visit each HEI in the country to collect the data. Therefore, the actual number of participants in the survey were some of the computer students and tutors in the participant institutions as follow:**

- 1. In the preliminary data gathering stage, a total of 150 participants (120 computer science students and 30 staff) took part in the survey (as described in Chapter four)**
- 2. In the follow up experimental evaluation of the m-learning security framework, a total of 13 participants; comprising 5 computer science students and 8 academic staff were involved (as described in Chapter six)**
- 3. In the design and evaluation experiment of the m-learning security enhancement app, a total of 125 participants (110 computer science students and 15 academic and non-academic staff) are engaged (as described in Chapter seven).**

3.5 Data Analysis

In this research five data collection experiments were carried out at different stages of the research. The analyses of the data for result generation were dealt with based on their nature of either being quantitative or qualitative. The methods applied for the analysis such as statistical tests are described in this section. Throughout this thesis, descriptive statistics were conducted to analyse quantitative data obtained especially in the preliminary survey. The data from the design experiments was mainly qualitative, therefore a qualitative content analysis method was employed. The summative approach of the qualitative content analysis was used as it focuses on collecting themes that hold the main themes for the interview questions. These themes are collected from the raw data generated by the users and further analysed within the underlying context. Details on the analysis of the use of this method are found in Chapters four, five, six and seven which analyse the results of the preliminary study, m-learning security framework and design of the intervention application.

The questionnaires were designed with single choice, multi-choice and Likert scale between one to five, with one being the lowest and five being the highest, depending

on the context of investigation or evaluation. Most of the Likert scale are used to indicate the extent of their agreement or disagreement with a given statement. A five-point Likert scale usually ranges from 'strongly disagree' (1) to 'strongly agree' (5) with a corresponding neutral midpoint. Details on usage are given in their respective chapters.

The validity and credibility of the quantitative and qualitative data collected must be guaranteed by using descriptive statistical analysis and appropriate statistical tests (Rugg, 2007). In this thesis percentages, rates, tables, charts and graphs are used for grouping and analysing the data in accordance to their relevancy. In the chapters where it is necessary to ascertain if some sets of data are significantly different, it is necessary to apply a statistical hypothesis test. The chi-square statistical tests for dependency are performed on the data obtained in this study with the significance level at $p \leq 0.05$ (which is the normal significance threshold used in statistical significance research studies). In addition, the Mann-Whitney U test which is a nonparametric test, has also been used in some of the findings and evaluations found in chapters five, six and eight.

3.6 Research Ethics

The University of Warwick Biomedical and Scientific Research Ethics Committee (BSREC) requires that any research study that involves the participation of individual must follow certain guidelines on ethical practice. Therefore, before any of the surveys were conducted, ethical consent was applied for by the researcher and approvals were granted by the relevant bodies (The participating institutions or departments in Nigerian HEI and The University of Warwick Biomedical and Scientific Research Ethics Committee reference (REGO-2013-472 and REGO-2016-1768). A thorough ethical consent process was followed during the surveys which was supported by the required consent forms. In the ethical applications for this

study, details were provided on the research process and objectives, participants' security and confidentiality, an assurance of data security, providing evidence that none of the research activities and processes could bring any harm to participants. The following are also adhered to in addition to the BSREC ethical rules.

Privacy Issues: Information on participants' private and social media activities such as internet browsing, emails, education and other social media undertakings are somehow connected with some survey questions in this study, it is therefore appropriate for the researcher to keep with upmost confidentiality responses gathered from this research.

Anonymised and optional Participation: Participant responses are sought voluntarily and kept strictly confidential in order to obtain their unbiased opinion on the collected data. Therefore, only interested participants were invited to take part in the study randomly, this will ultimately bring out their impartial view on the research investigations. Furthermore, the institutions and participants in the study were made aware of the followings in clear terms through the participant information leaflet:

- (i) The aim, purpose, process and timing of the research;
- (ii) Any risk(s) that can be identified within the research activities;
- (iii) An assurance that the confidentiality and anonymity of the participants will be protected;
- (v) A guarantee that the participants are allowed participate freely in the research process and so has the right to withdraw their participation any time;
- (vi) An assurance that the participants have the right to request for a copy of the research results after 30 days;
- (vii) That the participants can only take part in the study after signing the consent form provided.

3.7 Summary

This chapter begins by reflecting the basis on how the research in this thesis was conducted. It introduced the research methodological approaches which were followed to establish the answers to the main research questions and objectives. For the purpose of this research, literature review has been used from the beginning in order to understand the underlying problems and keep abreast of the current happenings in the area of research. Having gathered relevant background information, the user-centred methodology was adopted and used throughout, in the preliminary investigation, design and evaluation stages. ISO standard 9241 -210 and Technology Acceptance Models are the bases for the adoption of UCD approach due to its emphasis on the need to explore needs of users in the iterative and incremental development application process. While other evaluation techniques were considered, the user centred evaluation approach is employed in this research to assess the system's usability, usefulness and accessibility. This chapter also discussed the methods of data collection mainly, quantitative and qualitative techniques, the data analysis methods employed and used as evaluation tools, sample size and sampling method adopted in the research as well as guiding ethics, in order to provide a blueprint for the overall research.

CHAPTER IV

Users' Experience – Findings, Evaluation & Validation

4.1 Introduction

This chapter introduces the primary research study conducted to identify the major security concerns and issues being faced by users of mobile learning in tertiary institutions in Nigeria, particularly the students and teachers as discussed in chapter two of this study. Thus, the chapter explores the users' experience on security issues when using their mobile gadgets for learning purposes through the primary study conducted at the beginning of this research in 2013. This research is necessitated by the fact that the researcher needs to identify the problems that students currently faced when learning using their mobile devices and to confirm the problem statement presented in the introduction of this study. The study involves academic participants, starting with the academic tutors to students and other stakeholders such as the managers of the education institutions and non-teaching staff. Before going into the details, the rationale for embarking on the study is described below.

Along with several opportunities in m-learning which were discussed in detail in chapter two come some challenges that need to be addressed. There are concerns that arises from the use of mobile devices for learning and teaching purposes that may affect m-learning adoption negatively. Some important concerns about the use of mobile devices in learning is the security risk and vulnerability attack issues relating to educational content and private information of the stakeholders. Pervasive use of m-learning may entail, among others, loss of privacy, and attacks on users and institutional security in terms of integrity, confidentiality, and privacy of the users' data who are involved in the learning process. Higher Education Institution management, educators, and individual learners are profoundly worried about the growing security threats in m-learning. Security risks such as unauthorised interference with the learning content and instructions by the learners is a concern

among educators and education providers. More importantly, as students are allowed to use their portable devices to access learning content and materials anywhere, this increases the security risks. On the other hand, students' records, e-portfolio data, assessment results and feedback are some examples of information that need to be safeguarded for the students' sake.

Therefore, the challenge is to safeguard what should be learnt in the lecture room, what should be learnt outside the classroom, and the methods in which connections between these two settings should be made (Hashemi *et al.*, 2011). The focus of this chapter is to examine mobile learning security from the users' experience, and determine the areas of safeguarding and protecting the privacy and security of individual data, systems and equipment. *Thus, this chapter aims to answer RQ2 on the users' experience on m-learning and the security issues they might encounter when using devices for learning. The following sub research questions are designed to help find the solutions.*

4.2 Survey Questions

The survey questions are grouped under different stakeholders: students, academic tutors, and other stakeholders such as education providers and administrative staff as below.

4.2.1 Students' Perspectives

RQ 4.1 How important do students consider the security of their mobile devices?

RQ 4.2 What security concerns may students have when using their mobile device for learning?

RQ 4.3 How are the students being affected by m-learning security threats?

4.2.2 Academic Tutors' Perspectives

RQ 4.4 What are the lecturers' concerns on security issues that might affect m-learning in Higher Education Institutions in Nigeria?

RQ 4.5 How are the tutors/lecturers being affected by the security threats in m-learning?

4.2.3 Institutions and Other Stakeholders

RQ 4.6 What are the m-learning security issues that stakeholders may face?

RQ 4.7 How are the institutions being affected by the security threats in m-learning?

4.2.4 General

RQ 4.8 Who among these stakeholders are most affected by the security issues?

RQ 4.9 What are the responsibilities of the stakeholders in ensuring risk free m-learning?

4.3 Methodology

In identifying and understanding the security challenges of mobile learning in Nigeria HEIs, the study employed a survey based on a user-centred methodological approach using **a sample population of computer science students** and lecturers and instructors in the four universities mentioned in chapter one. Thus, the students and the teachers are the focused participants, since they are the main users. The researcher also believed that due to the students' and lecturers' involvement with m-learning, they possess a good understanding of the problems either through personal engagements or experience. In order to ensure greater accuracy and reliability than a single method of data collection and analysis, two separate research activities were

carried out as primary instruments for quantitative and qualitative methods to gather the data. Therefore, this methodological approach makes use of mixed methods which is a combination of several research methods being used in the same study in order to ensure that the instruments complements each other and to allow comparison of the outcome from the analysis of the data. Both qualitative and quantitative methods were used for the purpose of triangulation and the researcher is of the opinion that by engaging the two methods data collection and analysis, the credibility of the interpretation of the data and the subsequent findings are enhanced as evidences emerge from two different sources. While the questionnaire is the instrument used for quantitative method, the semi-structured interview is the instrument for qualitative methods.

4.3.1 Student Questionnaire Survey

In finding solutions to the research questions, primary data were collected on security issues being encountered by learners in four universities in Nigeria. The data collection method involved delivering a set of questionnaires to 120 **computer science students**. The questionnaire, which was made available to the participants both online and paper-based, was found to be the most suitable method to collect the required experiences from users who engage their mobile device for learning purposes. The instrument for the data collection was divided into four sections. The first section of the questionnaire-1 (See Appendix 1) was designed to understand the demographic background of the students, covering gender, age, course studied and university. Section two gathered data on various mobile devices owned by the participants, the type of activities they are used for and how often they download or install apps on their devices. Section three covered general questions regarding the respondents' awareness on m-learning technologies, the types of learning activities they engaged with their devices. It also asked the participants if using a mobile device for learning improves their academic performances and whether they will continue to use mobile device for learning on a regular basis. Part four was based on security

aspects of m-learning systems. It obtained data on user' concerns on m-learning security, how the security of m-learning systems is breached and the effects of security breach to them. The section also gathered data on how to reduce attacks on m-learning system. **Technical terms and concepts were explained briefly in the questionnaire and the researcher was available during the study to assist the respondents in understanding any part of the questionnaire.**

4.3.2 Teachers' Interview

The second instrument for data collection was a series of semi-structured interviews were conducted to answer the research questions discussed with teachers from the Information System and computer science departments from the four participating universities (See Appendix 2). The interviews are useful in verifying the security and other related problems when adopting and using m-learning in Nigerian HEIs and in finding out participants' experience which cannot be measured by questionnaires only. Thus, this descriptive method was also chosen because it suits the aims of this chapter to collect opinions about the experience of the users. The interviews highlighted some of important issues for the above research questions which are not specifically stated in the questionnaire as they may require considerable expertise and experience to answer. The interviews which were conducted with 30 teachers were divided into three parts. Part one was an introduction, explaining the purpose of the interview to the participants and also to collect some demographic information while assuring them anonymity. Participant Information leaflets and consent forms were distributed and returned at this introductory stage. Part two dealt with the general question on m-learning regarding awareness, adoption and implementations. It also dealt with the acceptability and usability of m-learning as a learning, teaching and assessment approach. Part three was the main section diving into issues surrounding m-learning. The research study was conducted at four universities from South West Nigeria using qualifying demographics such as gender and age. Secondary instruments for data collection are documented evidence, unpublished papers and

articles obtained from the academics and administrative staff as well as information obtained through research papers from relevant journals which were used to support the primary data gathered from the research study.

4.4 Pilot Study

Before the field study was carried out, a pilot study was arranged and conducted with a small group of participants who are PhD candidates in the Computer Science Department at Warwick University to review the questionnaire and mock interviews were also conducted. Opinions and suggestions given by them were taken into consideration in making the final copy of the survey. A pre-test was conducted for the second time with another group of colleagues in order to ensure high reliability and understanding of the questions. In all instances of the survey ethical approval was sought and obtained through the authors' university which is enough to carry out the study without getting further ethical approval from the participants' institutions, however individual consent was obtained from all the respondents by signing the consent form and they were assured anonymity. The data from the pilot stage were not used in the main study.

The data were analysed using relevant statistical approaches, a detail on this has been given in section 3.3.2. For the purpose of triangulation and to improve the credibility of the interpretation of the data, the findings from the questionnaire study were cross validated with findings from the qualitative study process. The data were analysed using relevant themes to aid the author to establish patterns and answer the research questions presented in this thesis. In the themes or keywords where some of the participants' understandings expressed by the members to indicate their opinions on the subject matter.

4.5 Analysis of Results

The findings of this research are organised into nine sections in order to provide answers to the survey questions as shown below. Being the largest number of participants, students' demographics such as age group and gender, were used in analysing the results.

RQ 4.1: How important do students consider the security of their mobile devices?

This question **relates to survey questionnaire number 11** and it is to determine how important **computer science students** consider the security and safety of their handheld devices - mobile phones, smart phones, tablets and other handheld devices they used for learning purposes. It is to find out if the students who are the focus of this study consider or do not consider the security of their device important. The question is a single choice and all 120 students responded. Over two-third of the participants (70.88%) indicated that the security of their device is 'very important' to them, 26.57% pointed out it is 'important', and only 2.55% said it is 'neither important nor unimportant' to them and 0% said it was unimportant. Considering the gender distribution, 69.84% of the female and 71.93% of the male students indicated that their mobile devices are very important to them. 28.57% of the females and 24.56% of the males responded that their mobile devices are important to them, as shown in figure 4.1.

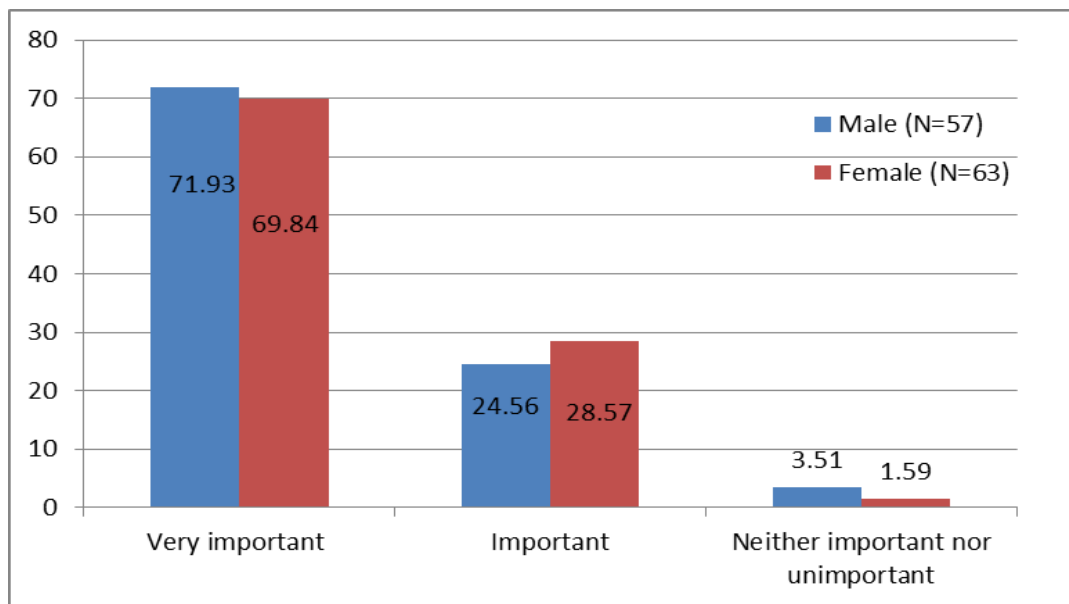


Figure 4.1: How important students consider the security of their mobile devices?

There are various reasons given by the participants as why the security of their m-learning devices is important to them, some of which are highlighted in the discussion section.

RQ 4.2: What security concerns students may have when using their mobile device for learning?

This research question relates to questionnaire number 14 in the survey to determine computer science students' security concerns. Approximately six out of ten of the participants (62.5%) considered theft/loss as a concern which may indirectly leads to loss of learning content if landed on the wrong hand. **75% indicated unauthorised access to mobile device used for learning is a concern has it may lead to an unauthorised access to learning contents or instruction. This is possible when colleagues and friends used their handheld device without their permission, which is a source of worry to some participants.** Nearly seven out of ten of the participants (65.2%) indicated that virus or malware attacks are inevitable and it is a form of concern when using a mobile device for learning while nearly a

third of the participants (29.17%) said ‘denial of service’. Figure 4.2 shows the demographic information on security concerns students may have on m-learning based on gender.

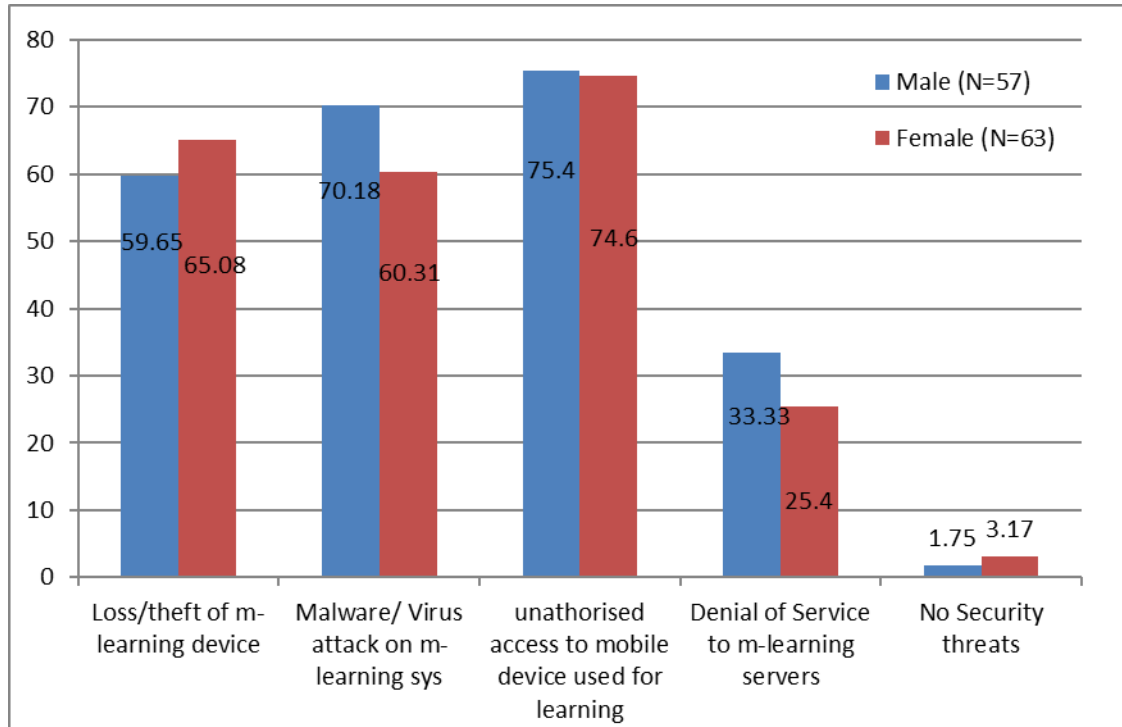


Figure 4.2: Security issues learners may encounter in m-learning

On a gender basis, 65.08% of the female and 59.65% of the male indicated theft or loss of device, 74.6% of the female and 75.4% of the male indicated unauthorised access to mobile device used for learning purposes. 60.31% of the females and 70.18% of the males responded that virus or malware attack is a concern to them while 25.4% of the female and 33.33% of the male noted denial of service.

RQ 4.3: How are the students being affected by the m-learning security threats?

This research question relates to questionnaire number 16 in the survey. A large numbers of **computer science participants** said they are affected by m-learning security threats which include loss of confidential or personal information in the

event of breach. This observation accounted for 79.70% of the participants. Loss of study hours and loss of performance accounted for 71.68% and 65% respectively. Psychological effects resulting from security breaches of mobile devices accounted for 46.62% while two students indicated that they have not experienced any damaging effects as a result of security breach. Figure 4.3 shows the demographic information on the damaging effects of security.

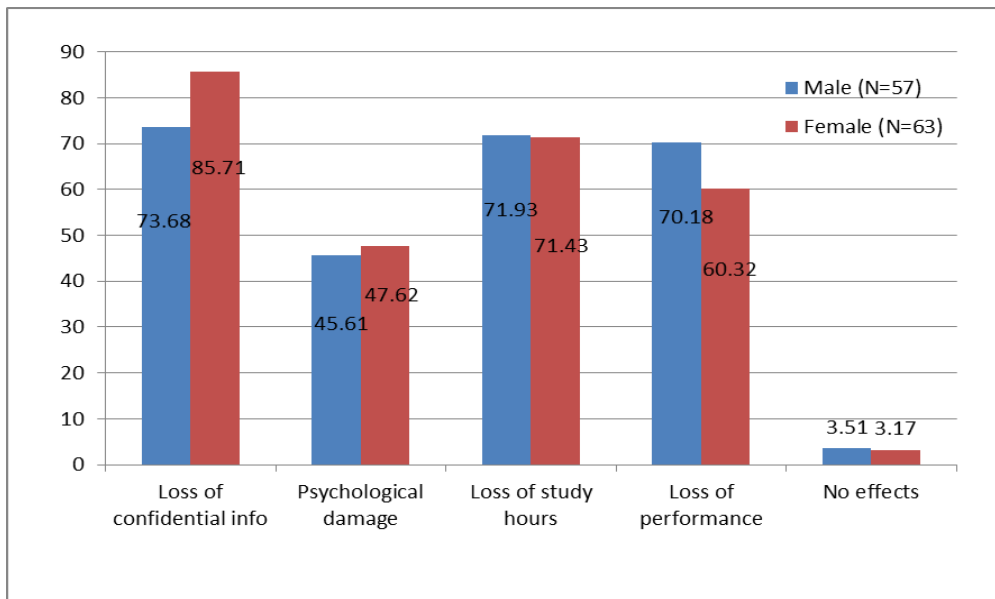


Figure 4.3: How the students are being affected by m-learning security threats

Based on gender difference, the most common effect of m-learning security to students in HEIs in Nigeria is loss of confidential or personal information as indicated by 85.71% of the female and 73.68% of the male. 71.43% of the female and 71.93% of the male respondents feared loss of study hours as the effect of a security threat. Similarly, 60.32% of the female and 70.18% of the male students indicated loss of performance in learning as security risks. Psychological effects resulting from security breaches of mobile devices account for 47.62% of the female and 45.61% of the male students respectively.

NOTE: While the questionnaire asked “What do you think are the damaging effect(s) of mobile learning security threats to the students?”, the researcher was present during the survey and asked the participants to complete the questionnaire including the question 16 based on their experience on m-learning and not what they think (as written in the questionnaire) because the questionnaires have been printed and taken to survey field before the mistake was noticed.

RQ 4.4: What are the lecturers’ concerns on security issues that might affect m-learning in Higher Education Institutions in Nigeria?

This research question relates to interview question 7 in the survey and it addresses security issues lecturers may encounter when using mobile devices as teaching aids, as the experience of the lecturers remain very important in the adoption, implementation and use of any mobile innovation in the education system. Top on the list are privacy issues and students exploiting a security breach to perpetrate malicious acts, followed by data interception to commit illegal or fraudulent activities. 76.6% of the educators acknowledged that privacy issues and exploitation of security breaches are concerns to them when using mobile devices for teaching. Another 53.3% of the educators indicated that interception of personal and confidential information by students and outsiders, either for fun or malicious acts, is a security threat for them. Over 65% of the educators feared unauthorised access to learning content and unpermitted sharing of copyrighted e-materials by the students among themselves as security issues being perpetrated by learners in HEIs in Nigeria through mobile devices, this is made possible due to lack of copyright laws and software piracy in Nigeria (Wazir, 2011; Obodoeze *et al.*, 2013). 60% of the educators were also concerned about virus and malware attacks on m-learning systems. 46.6% of the educators acknowledged that denial of service is a security risk to the m-learning environment while 36.67% of them are of the view that propagation

of false or misleading information using mobile devices among the learners is a threat to m-learning. This is quite common as some students spread incorrect information through social media (Jegade, 2009). However, 6.67% of the educators indicated that m-learning poses no security threats to them when using mobile devices as a teaching aid or that any issues posed by the devices can be overcome successfully.

RQ 4.5: How are the tutors/lecturers being affected by the security threats in m-learning?

This research question relates to the second part of interview question 7 in the survey which is to find out how security threats affect the tutors. The educators indicated many risks such as loss of confidential information, unauthorised change in learning content, loss of control during e-examinations, loss of privacy, as well as psychological effects. Around nine out of ten participants (93.3%) indicated that loss of confidential information is a major consequence of the m-learning security threat to educators while more than eight out of ten participants (86.67%) indicated that loss of control mainly during e-assessment and online examinations is a threat to the academic staff. Also, more than eight out of ten (83.3%) agreed that loss of content quality of learning materials is a concern while exactly three out of ten indicated psychological effects as a consequential result of m-learning security threats. Almost half of the participants (48%) indicated that loss of privacy is a security threat to m-learning for the academics. These statistics are summarised in figure 4.4 below.

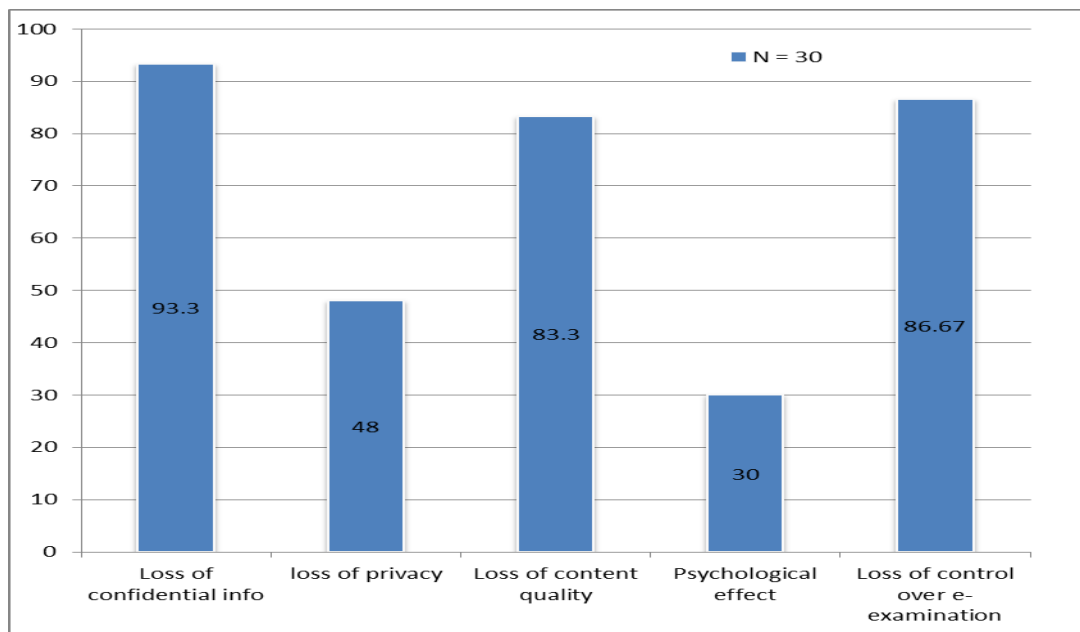


Figure 4.4 How educators are being affected by m-learning security threats

RQ 4.6: What are the m-learning security issues that stakeholders may face?

The research question is a multi-choice question to find out various security issues stakeholders might have encountered when using mobile devices to complement teaching and learning activities. Figure 6.5 shows the various security issues and topping the list is unauthorised access to learning content and materials (75.6%), followed by virus/ malware attack on m-learning system (68%). Denial of service is considered the least important threat to m-learning systems (30.5%). **This question combined the responses of the students, tutors and some administrative staff and it relates to questionnaire number 17 and interview question 7.**

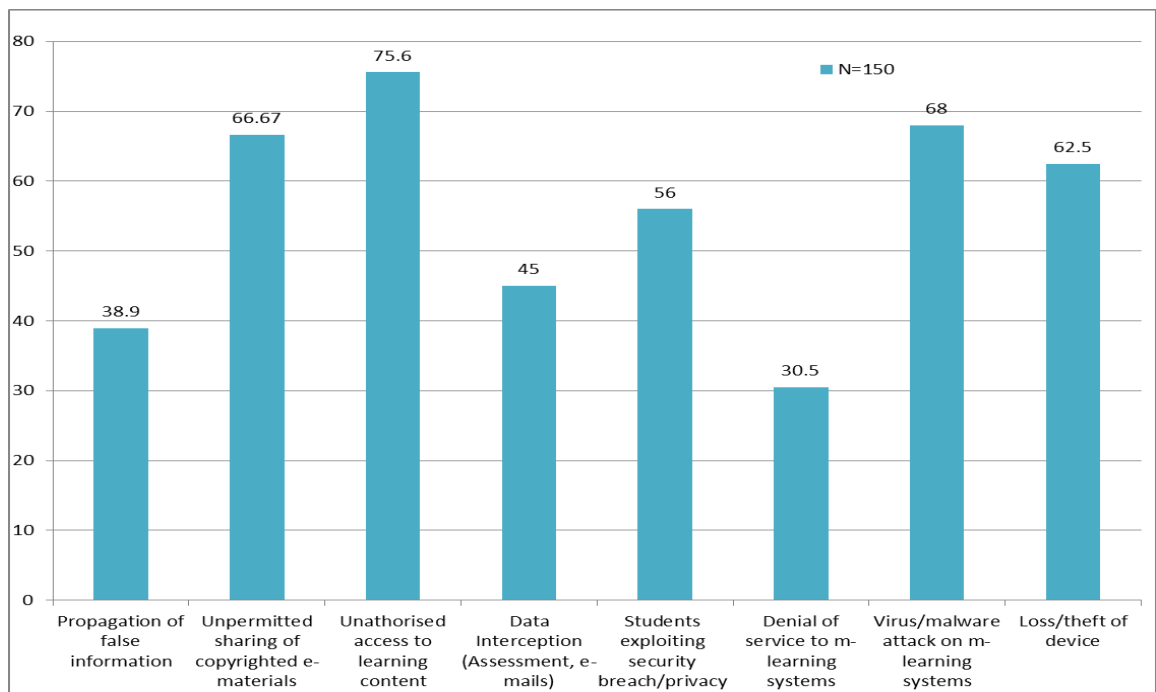


Figure 4.5. What are the m-learning security issues that stakeholders may face?

RQ 4.7: How are the institutions being affected by the security threats in m-learning?

This research question relates to questionnaire number 18 and interview question number 6. This part of the survey investigated the adverse security effects of m-learning on the HEIs who are interesting in incorporating m-learning in their curriculum. Educational institutions and their management are stakeholders in knowledge development and delivery, and they risk suffering loss of confidential information, reliability, and goodwill, as well as working hours of the developers and support staff, to security issues as shown from the survey data. Around nine out of ten participants (87.78%) indicated loss of confidential information as the most adverse effect of security threats to m-learning for HEIs. Eight out of ten participants indicated loss of goodwill and integrity as the risk of m-learning threats to the HEIs. In case of a successful hacking, there is a loss of reliability on the part of the

institution which 77.8% of the respondents pointed out. 43.3% of respondents also indicated loss of working hours in correcting the anomalies, restoring students' confidence and rebuilding integrity of the institution after a security breach.

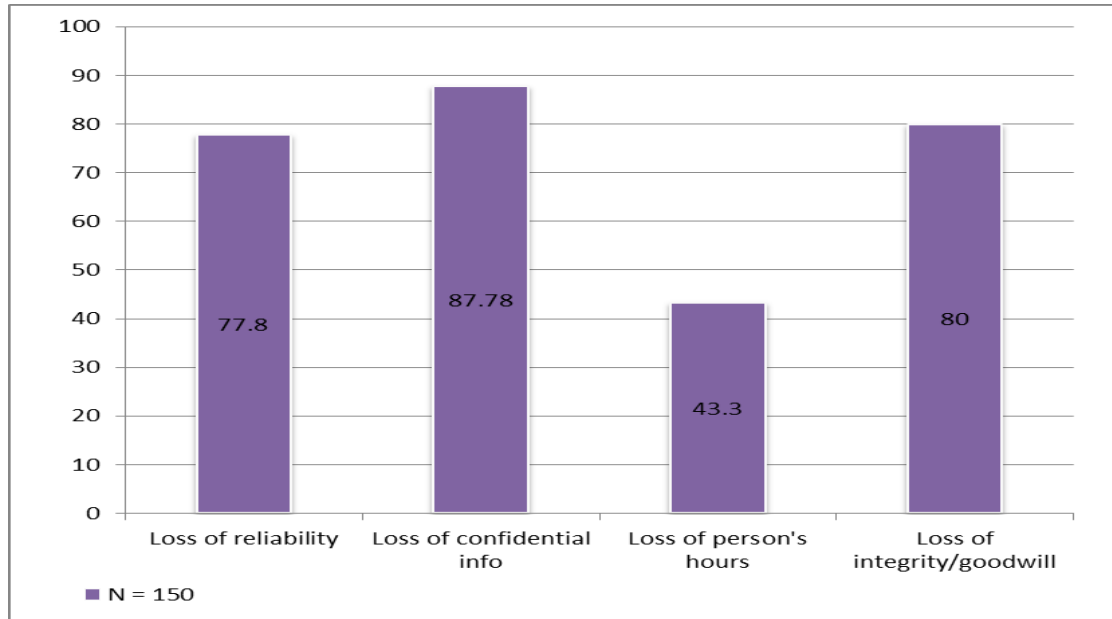


Figure 4.6. How educational institution are being affected by m-learning threats

RQ 4.8: Who among the stakeholders are most affected by the security issues?

This section of the study reveals that among the different stakeholders in a university community, the university management are most affected by any security threats. The faculty lecturers and students as users are also affected next, after the management. Figure 4.7 illustrates how the vast majority of respondents (66.67%) indicated that the university management and promoters are most affected by m-learning security threats among all the stakeholders. This is highly likely to happen as they are the policy makers in charge of the smooth running of the university. The lecturers and support staff are next as indicated by 53.33% of the participants. Students are affected as indicated by four out of ten participants. The developers are least affected and it may be due to the fact that m-learning systems are being developed by a consultancy

outfit or software company. **This research question relates to questionnaire 19 and interview question 10.**

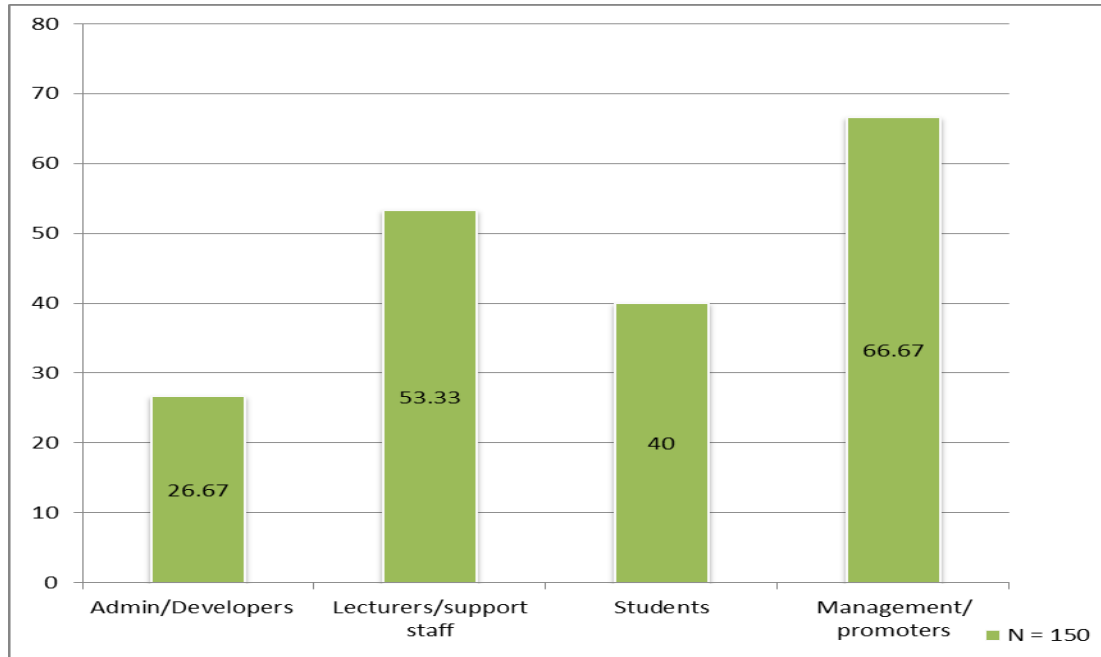


Figure 4.7. The affected stakeholders in m-learning

4.6 Statistical and Hypothesis Testing

Common statistical tests were carried out in further analysing the results obtained to establish some associations among the variables using the chi-square statistical test and Mann- Whitney U tests based on gender from the data collected from the students. We also tested for security issues from students' and educators' standpoints. For survey questions related to students only, we determine if there is a gender difference on:

- The importance of m-learning security to the students;
- The risks of m-learning to the students;
- The effects of m-learning security breaches to the students.

Thus, the following hypotheses were tested:

H1: There is gender difference on how important the students consider the security of their m-learning devices;

H2: There is gender difference on the risks of m-learning devices among the students;

H3: There is a gender difference on the effect of security breach among the students.

The first hypothesis was tested using the chi-square statistical test for dependency based on gender differences in order to determine the importance of the security of mobile devices to the students.

Table 4.1 How important do students consider the security of their mobile devices?

| Results: How important is the security of m-learning device for students | | | | |
|---|-------------------|-------------------|-----------------|-------------------|
| | Very important | Important | Not important | Row Totals |
| Female | 44 (44.62) [0.01] | 18 (16.80) [0.09] | 1 (1.58) [0.21] | 63 |
| Male | 41 (40.38) [0.01] | 14 (15.20) [0.09] | 2 (1.42) [0.23] | 57 |
| Column Totals | 85 | 32 | 3 | 120 |

The chi-square statistic was calculated as 0.6408, P-Value as 0.725852 at the confidence interval of 0.05. The test shows that there is no gender difference on how important the students consider the security of their m-learning devices.

The second survey question on the risk and security issues that students experience when using their mobile devices for learning, Mann- Whitney U test was used for the calculation as shown in table 4.2 and table 4.3 below.

Table 4.2: Ranking of female and male on m-learning security

| Gender | Participants | mean of ranks | sum of ranks |
|---------------|---------------------|----------------------|---------------------|
| Female | 63 | 5.8 | 29 |
| Male | 57 | 5.2 | 26 |
| Total | 120 | 5.5 | 55 |

Table 4.3: Mann- Whitney test on m-learning security

| Test | m-learning security threats |
|------------------|------------------------------------|
| U Mann - Whitney | 11 |

| | |
|------------------------------|----------------|
| Z | 0.2089 |
| Asump. Sig (2-tailed) | 0.83366 |

According to table 4.3, since the value of Z is less than 1.96, there is no significant difference between female and male students' experience in relation to the security threats in m-learning. This implies that there is no gender difference on the risks of m-learning devices and that both male and female observe similar security risks.

On the third survey question, the result was further analysed using the Mann-Whitney U test as shown in tables 4.4 and 4.5.

Table 4.4: Ranking of female and male on m-learning security effects

| Gender | Participants | mean of ranks | sum of ranks |
|---------------|---------------------|----------------------|---------------------|
| Female | 63 | 5.9 | 29.5 |
| Male | 57 | 5.1 | 25.5 |
| Total | 120 | 5.5 | 55 |

Table 4.5: Mann-Whitney test on m-learning security effects

| Test | m-learning effects |
|-----------------------|---------------------------|
| U Mann - Whitney | 10.5 |
| Z | 0.3133 |
| Asump. Sig (2-tailed) | 0.75656 |

The test shows that there is no significant difference in the hurtful effects felt by the students in the event of an m-learning security breach. This implies that both the male and female students experience the same effects on m-learning security risks.

For survey questions that are related to all the main stakeholders, further statistical analyses were carried out to compare the security issues and their effects on students and academic staff, the two focal users of m-learning systems. Thus, the following hypotheses were tested:

H4: There is significant difference between the students and educators on the security risks in m-learning;

H5: There is significant difference between the students and educators on the effects of m-learning security.

Table 4.6 and Table 4.7 below show the calculation of m-learning security issues that these users may face using a Mann-Whitney U test for dependency.

Table 4.6: Ranking of students and staff in m-learning security

| Stakeholders | Participants | mean of ranks | sum of ranks |
|-------------------|--------------|---------------|--------------|
| Students | 120 | 10 | 50 |
| Academics/support | 30 | 4 | 28 |
| Total | 150 | 6.5 | 78 |

Table 4.7: Mann- Whitney test on m-learning security threats

| Test | m-learning security threats |
|--------------------|-----------------------------|
| U Mann - Whitney | 0 (critical value of u = 5) |
| Z | -2.7608 |
| p-value (2-tailed) | 0.05 |

According to Table 4.7, since the value of Z is less than -1.96, there is a significant difference between students' and educators' experience in relation to the security issues that each set of stakeholders face in the use of m-learning. This implies that the educators and students have different views on the m-learning security issues and they are being exposed to different risks which may be due their different use of mobile devices in education. While academic and support staff use their m-learning for teaching and passing knowledge, the students use their m-learning devices for learning. These different standpoints are further explained in the discussion section. Furthermore, the Mann- Whitney U test was also performed on the data obtained regarding how the users are affected by the security threats in m-learning. The results of the statistical tests are shown in Table 4.8 and Table 4.9 below.

Table 4.8: Ranking of main stakeholders in m-learning

| Stakeholders | Participants | mean of ranks | sum of ranks |
|--------------|--------------|---------------|--------------|
|--------------|--------------|---------------|--------------|

| | | | |
|-------------------|-----|-----|----|
| Students | 120 | 7 | 35 |
| Academics/support | 30 | 4 | 20 |
| Total | 150 | 5.5 | 55 |

Table 4.9: Mann- Whitney test on main stakeholders

| Test | m-learning security effects |
|--------------------|--------------------------------|
| U Mann - Whitney | 5 (critical value of $u = 2$) |
| Z | -1.4623 |
| p-value (2-tailed) | 0.05 |

According to Table 4.9, there is no significant difference between students and academic/ support staff experience in relation to the security effects on stakeholders in m-learning. This implies that both stakeholders are exposed to the same or similar security risks when using m-learning. This assertion is factual because, being stakeholders, they both suffer loss of confidential information and privacy as well as psychological effects. In addition, academics and support staff are likely to suffer loss of control over e-exams and content quality while the effect on students are likely to include loss of study hours and performance.

4.7 Discussion

Most of the participating students said that the security of their mobile devices is important to them according to the result obtained above. **This study confirms that many computer science students in Nigeria HEIs** take the security of their mobile devices seriously and this is expected considering the usefulness of handheld devices in day to day activities as every student carries at least one mobile device. Many reasons are given by the students for taking the security of their mobile device seriously, the first reason being that mobile phones and smartphones are considered to be a valuable personal property, consequently they attempt to keep them safe. Many learners **in Nigeria HEIs** use their handheld devices to exchange education-

related messages and learning contents with classmates, search the internet and library databases for learning materials, and hold group discussions with classmates. Therefore, **computer science students in HEIs in Nigeria** understood that their mobile devices are vital to their academic success and they are mindful of the security of their mobile devices.

Furthermore, many **computer science students in Nigeria HE** also use their handheld devices as data storage, thus they have their personal information on them. Consequently, having mobile security awareness is an important aspect of protecting their privacy. This result is supported by the work of Kambourakis (2013) that discusses the security and privacy challenges of m-learning and suggests that learners are extremely concerned about the security and safety of the data they store on their mobile devices. Also, **one of the educators stated during the interview that “a mobile device is important as it can be adapted for learning by using it to send materials to students and using it for online assessment and receiving feedback, therefore the security of such an important tool in education should be not taken for granted”**.

On security issues that users may encounter when using mobile devices for learning, a very high percentage of students (81.11%) indicated that unauthorised use of portable devices by friends or classmates of the owners as a security risk. The potential for unauthorised use of portable devices is suggested to be high among learners in **Nigeria HEIs** since they usually live in shared hostels, and mobile devices left on a table can be picked up by roommates and used for gaming or educational purposes. This act may lead to unauthorised access to confidential information of the owner since many students have personal details such as full name, address, date of birth, email address and even their bank account information on apps on their mobile devices. 76.6% of the educators acknowledged that privacy issues and exploitation of security breaches are concerns to them when using mobile devices for teaching. Another 53.3% of the educators indicated that interception of personal and

confidential information by students and outsiders, either for fun or malicious acts, is a security threat for them. **During the interview one of the educators stated that “The illegal activities of the students in Nigeria HEIs should be a top consideration. Most students are into cheating and tampering with personal information, their activities can be perpetrated through m-learning”.** This result is in line with the findings of Kambourakis (2013) in which system and data security and actors’ privacy are the first two challenges identified in m-learning.

Significant proportions of the risks are loss and theft of mobile devices. **These illicit practices are common among students in Nigeria HEIs** since mobile devices are still regarded as precious possessions, and in some cases where the HEI supplies learners with mobile devices, there are concerns about making learners attractive to thieves. This result is in line with Obodoeze *et al.*’s (2013) study which demonstrated the second most challenging security concerns affecting mobile users in Nigeria is the frequent or widespread losses of mobile device by their owners to thieves or the owners carelessly lose their mobile phones while in transit. It is also consistent with a survey conducted by Juniper (2011) on mobile device users that showed that one out of every three mobile device users has lost their device at some point in time.

Virus and malware attacks are also indicated as some of the threats when using handheld devices for learning purposes and they are normally encountered when downloading educational materials from an unknown source as indicated by some students, who are unaware of the present of malware downloaded with their materials. Some of them have also visited some game sites through which their devices got malware infected. Similarly, 60% of the educators were also concerned about virus and malware attacks on m-learning systems. This result is also consistent with the work of Obodoeze *et al.* (2013), which identifies the various forms of threats including virus/malware attack and hacking as the biggest security challenges being faced by mobile device users in Nigeria.

Access to information and group discussion as well as learning content and instructions, may be disturbed through a DoS attack if the network is penetrated. In addition, **DoS is a threat that results from irregular power supply to mobile learning servers, which is common in Nigeria.** This study is supported by the findings of Osang *et al.* (2013) in which 64% of the respondents identify that the poor power supply situation in the country is a barrier to m-learning. **During the interview one of the educators stated that “DoS may occur during unscheduled downtime due to maintenance of network infrastructure, which can lead to loss of connectivity between mobile devices and servers”.** It can also be caused by physical attacks on network infrastructure on universities campuses, which are common, for example during student riots in some universities in Nigeria. 46.6% of the educators also indicated that denial of service is a security risk to m-learning environment.

Another security issue which is a concern to over 65% of the educators is unauthorised sharing of learning content or unpermitted sharing of copyrighted e-materials by **Nigerian students** among themselves which is another form of unauthorised access made possible by weak e-copyright laws. Propagation of false or misleading information using mobile devices among the learners is a threat to m-learning according to 36.67% of the educators. This practice is quite common among Nigerian students as some of them have the habit of spreading incorrect information through social media (Jegade, 2009). However, 6.67% of the educators believed that m-learning poses no security threats to them when using mobile devices as a teaching aid or that any issues posed by the devices can be overcome successfully.

How the educational institutions, educators and students in **Nigerian HEIs** are affected by m-learning security threats are shown in Figs. 4.3, 4.4 and 4.6. A common effect among all stakeholders is loss of confidential information, leading to loss of privacy. 92.22% of the learners agreed that loss of confidential information is the most hurtful effect. This result is consistent with the work of Zamzuri *et al.* (2013),

which states that one of the reasons why students reject online systems is due to security reasons because they are worried about the loss of their private and confidential information. Similarly, 93.3% of the educators believed that loss of their confidential information is a major security consequence of m-learning. The study is consistent with the work of Kambourakis (2013) who states that loss of confidential information is one of the worries for lecturers in m-learning and their confidentiality should be guaranteed at all times. **In the interview one of the educators stated that “educators would want their identities to remain confidential to avoid falling victim to unsuspected criminals who can assume their identity to carry out malicious acts”.**

The study also reveals that 70% of **computer science students’ in Nigerian HEIs** feared loss of study hours and performance as consequences of a security breach in m-learning due to DoS, which is possible when learners view m-learning systems as a complement to the classroom and rely on it as one of their main learning platforms **in Nigerian educational context**. This implies that non-availability for a long period of time will have adverse effects on learners’ study hours, revision time and consequently their academic performance. This raises the worry that students may be reluctant to fully engage with m-learning and therefore fail to realise the full potential of m-learning to their learning experience because of their concerns about loss of study hours and performance in the event of a security breach. This finding is in line with the work of Kukulska- Hulme *et al.*(2009),which states that good m-learning improves learners’ study retention and performances in their study. **One of the participants in the interview stated that “learners need a reliable, highly available and dependable m-learning system to avoid being frustrated in the event of disconnection to the m-learning system, which can affect their study performance adversely”.** Some of the **learners in Nigeria** (47.62% of the female and 45.61% of the male) indicated that they are likely to experience psychological disturbance if their personal information is leaked through a mobile device or m-learning system or if their privacy is infringed. However, 3.33% of the learners stated

that a security loophole in an m-learning system poses no adverse effect to them because they have security awareness about the information they have on the mobile devices and they avoid as much as possible storing private information on their mobile devices.

In the interview most of the educators stated that the loss of control mainly during e-assessment and e-examination is a worry for the academic staff and a threat to adoption of e-learning in Nigeria. This can lead to examination malpractices and illegal collaboration during assessments if m-learning is not properly implemented. The educators' standpoint is consistent with a similar study conducted in Nigeria by Osang *et al.* (2013), in which most of the tutors believed that m-learning will ease examination malpractices. Again, our findings agree with that of Kambourakis (2013) which revealed that e-examination procedures carried out in an unsupervised or semi-supervised way is one of the difficult challenges within the m-learning context, as educators who are interesting in using any technology for educational purposes, will want to take ownership and control of such projects. **In the interview, some of the educators also acknowledged that loss of content quality of learning materials is a likely side effect of introducing m-learning system that can make it possible for learners to tamper with learning materials if the security is weak.** However, altering learning content and grades without authorisation and amending confidential documents may be possible if there is a security breach in the m-learning system known to the students. Thus, an m-learning system must be secured against manipulation and modification from legitimate users who are mainly students and from unauthorised users. Many educators interviewed indicated that they are likely to experience psychological disturbance if their personal information is leaked through an m-learning system or if their privacy is infringed. However, 30% of the educators stated that m-learning poses no adverse effect to them in discharging their teaching delivery due to the fact that they take adequate precautions when using their mobile devices and use these as teaching aids (Lane, 2014).

RQ 4. 9: What are the responsibilities of the stakeholders in ensuring risk free m-learning?

Having identified and discussed the m-learning security issues that students, lecturers and other stakeholders may face, and how they are being affected by the security threats **in Nigerian educational context**, it is a common sense to note that the responsibility of ensuring a risk free m-learning environment lies mainly with the stakeholders themselves as they are the people involved in managing and using the system. Their collective responsibilities in ensuring risk free m-learning are highlighted below. **This research question relates to interview question 11.**

Educational Institution/Management: The education providers have the main responsibilities of running risk free m-learning systems. The research findings indicate that 81.8% of the respondents agreed that the university management is responsible for ensuring a risk free m-learning environment as part of their responsibilities as education provider. The university authority is the policy maker and also accountable for smooth running of the university facilities including m-learning infrastructures. Therefore, the educational institutions/ promoters can ensure risk free m-learning by performing the following steps.

- Create security awareness among other stakeholders and encourage them to be security conscious when using their mobile devices. Students should be made aware of the potential risk of connecting to bogus free Wi-Fi which criminals may have set up in public places in order to collect personal data. Creating security awareness is vital as our study revealed that some users do not take the security of their mobile devices very seriously, so there is a need to promote mobile security education among users. With adequate knowledge, students will be more security conscious about the safety of their handheld devices, thereby reducing the rate at which small electronic gadgets are lost or

stolen which is mainly due to their negligence. Creating awareness to reduce the threats among the students is also supported by 21 out of the 30 academic participants. **One participant stated in the interview that “Although m-learning security threats are quite worrisome, particularly among learners, some of the threats can be eliminated by giving security education and awareness to the students”.**

- Possible implementation of separate wireless networks for academic users and visitors, to access the internet from their mobile devices whilst allowing restricted access to m-learning systems. This is to ensure that m-learning users have access only to their required or legitimate activities on the system and reduce unnecessary traffic to the servers. This practice is quite common in foreign schools and universities but not in place at the universities where this research was carried out. Having separate wireless networks for learners, and visitors, to access the internet from their mobile devices will reduce the risk of users introducing viruses, accessing systems and data they should not have access to, unauthorised downloading and heavy usage degrading network performance (GSMA, 2012).
- Implement mobile device management (MDM) systems for administering the m-learning devices in real-time, in order to locate, track and gather information on the movement of the connected devices. This will also aid remote diagnosing and fixing of software security problems, installing and updating software on devices as well as erasing data on lost or stolen devices. Using MDM on institutions devices was discussed and supported by (Kambourakis, 2013; GSMA, 2012) as one of the ways to have control and monitor device usage activities, this however, may have negative effect on privacy of the users.
- In tackling the sharing of copyrighted e-materials, the university administrators can implement Digital Rights Management (DRM) solutions. DRM is a technology that can be used for content protection in m-learning

environment. It is a class of access control measures that are used to limit the use of digital content and devices. A DRM based m-learning system can focus on learning content protection and other basic procedures of m-learning facilities that can be secured. Use of DRM tool is supported by many of the tutors who participated in our study (63%) as one of the solution to reduce the prevalent sharing of materials without permission or regard for copyright, mostly among students.

- Modern biometric security measures like fingerprints, voice recognition, dynamic signature features and facial features which are already present as part of security features on some mobile devices can be very useful in m-learning for enabling post authentication and authorisation security. A very high number of the academic participants, about 80% or 24 out of the 30 were in support of the modern biometric measures as one of the ways to reduce m-learning security.
- The university administrators can also operate a blacklisting method whereby websites or categories of websites deemed to be inappropriate or insecure are blocked from the university's network. This intervention is known to work well in conjunction with MDM in foreign schools and educational institutions (GSMA, 2012), however, it is only possible on devices owned by the institutions.

Academic staff: Around four out of ten (41%) of the respondents indicated that faculty are also responsible for ensuring risk free m-learning as they are in charge of running the academic programmes including the m-learning as part of learning curriculum. The academic staff can ensure risk free m-learning through the following.

- Align the existing curriculum for m-learning with proper consideration for security as well as integrate new technology into their modules in a secure manner. This is important as alignment of the current curriculum into m-learning while putting security into consideration as being identify as one of

the challenges of mobile learning in **Nigerian HEIs** as indicated by almost six out of ten of the participants (57.33%).

- Participate in the design and development of m-learning systems and mobile apps for their taught modules and research activities and provide experts' opinions and contributions for the overall implementation and application of m-learning systems, in particular to their field of knowledge and research. Data from the survey shows that a large number of the academic staff (70%) mainly from computer science department are willing to take part in the development of m-learning system for their respective university, thus developing m-learning systems or apps in collaboration with academic tutors will be highly important in building and developing robust and secured m-learning environment.
- Computer Science academic staff can develop a highly secured m-learning system following a standard security framework for implementation and participate in training the support staff on security concepts such as data encryption. **One participant during the interview stated that “System security including mobile is one of the branches of computer science, therefore involvement of computer science staff in the development of security framework should be a priority”.**

Administrative/ Support staff: The responsibilities of support staff in ensuring risk-free m-learning include the following.

- Ensuring regular data backups are taken, installing firewalls on m-learning servers and having up to date anti-malware and anti-virus software installed on m-learning systems as well as installing all security patches. The general census among participants is that regular backups and having up to date antivirus will promote risk-free m-learning environment. While 72.2% of the participants indicated that regular backups will reduce security threats, 56.7% indicated that threats from malware can be reduced by having up to date anti-malware installed.

- A participant stated that **“Putting in place proper security procedures and policies that will prevent hacking activities which may deny legitimate acts”**, therefore a scheduled maintenance policy for m-learning servers and network infrastructure, as well as an uninterruptible power supply is a necessity. One of the solution for alleviating m-learning issues in relation to privacy and security breaches, as suggested by 83.3% of the educators, is having good security policies and measures in place in mobile learning systems.
- Provision of robust access control mechanisms for authentication and authorisation before permission is given to view or download learning content and materials. This further includes encryption of data on m-learning servers to safeguard learning content from unauthorised copying and downloading, and protect examinations, assessment and feedback processes from attackers and impostors. This recommendation is supported by large number of the participants (59.1%) that good security technological measures such as a reliable access control for authentication will reduce the security threats in Nigerian HEIs.

Students: In view of **computer science students’** concerns on m-learning, the following recommendations are offered for secure and effective m-learning.

- Our study revealed that, while most of the students considered the security of their mobile devices as very important or important, some of them do not (see fig 4.1 above). If some learners do not consider the security of their device important, therefore, the first task in alleviating security issues in relation to students is to promote mobile security education among users. With adequate knowledge on possible threats and risks that they are taken, students take the security of their handheld devices more seriously.
- Security consciousness should be encouraged among learners who connect to educational resources while on the move using any free available WI-FI. While some students may not consider connection to free WI-FI a major

security threat, in some cases it may pose significant risk, they should avoid connecting to unsecured public Wi-Fi as many of them connect to educational resources while on the move using any free available Wi-Fi. They should be aware of the credibility of the organisation providing the connection regarding the security and safety of free network facilitates before using it. For example, connecting to an unsecured and unverified wireless infrastructure increases the chances of putting personal data at risk (Brody *et al.*, 2013).

- Security apps such as phone finders should be installed on mobile devices to enable locating them in case of lost or theft. Remote wipe apps should be installed to prevent unauthorised access to confidential and private information as well as learning materials stored on the devices if a lost device cannot be traced. This recommendation is supported by 58.9% of the participants that security apps should be installed on devices and in case of stolen, a remote wipe of data may be used to protect access to vital information stored on the device.
- Mobile devices should not only be secured with device locks; files should also be encrypted if sensitive information is stored on them. However, data encryption should preferably be used in combination with other security measures and in case other protective measures failed, encryption will ensure that even if a hacker manages to gain access to sensitive data, the format will not be readable. This recommendation is supported by majority of our participants, (73.3%) indicated having data encryption on the device will improve security.

4.8 Summary

While the use of mobile educational technologies for academic purposes may not increase the risk that may already exist as a result of learners' personal ownership of mobiles, the designers and practitioners of education are, however, responsible for producing coherent and reliable accounts of the likely consequences of the

proliferation of mobile devices in the higher education landscape. University staff already have demanding careers in knowledge delivery and expanding research, their privacy and confidential information being exposed in the course of discharging their duties should will be a concern if adequate security measures are in place in the m-learning systems. Similarly, loss of control during e-examinations and loss of content quality should neither be a concern nor source of worry for educators in a highly secured m-learning environment.

Learners studying **computer science in Nigerian HEIs** are also concern about m-learning security since they are the main users of m-learning. Therefore, adequate security education and awareness in form of tutorials and tips should be put in place for the learners in order to reduce the security palaver and give them confidence in using such technology. Furthermore, education providers and managers should focus not only on developing and using m-learning content and infrastructure but also make effort at securing the system because the users need a reliable, highly available and dependable m-learning system to avoid being frustrated when using the system.

In the next chapter we shall examine the common attack vectors (routes) of m-learning system in **Nigerian Higher Education Institutions**. We shall also identify which of the m-learning components is most prone to attacks or threats, is it the client, server or network component of the sub-frameworks.

CHAPTER V

M-learning Attack Vectors

5.1 *Introduction*

In the previous chapter, we introduced the primary research conducted in this study to identify the fundamental security concerns and users' experience in m-learning security. We explored stakeholders' understanding on m-learning security and the various risks that students and tutors have experienced on m-learning and came up with some recommendations on how to overcome some of the issues. In this chapter we will examine how threats may penetrate into the m-learning system and network environment. Thus, we are going to investigate the m-learning attack routes, since a typical m-learning system consist of three components which are the mobile device, one or more servers and network devices. One of the objectives of this chapter is to identify which of the components is commonly attack and how the security of m-learning devices is breached in Nigerian Universities based on user' experience. Thus, this chapter aims to provide solutions to RQ 1 on the threats to m-learning in HEIs in Nigeria and sub-research questions on the common attack route or components of m-learning in HEI in Nigeria and how the security of m-learning devices is breached or compromised. Before diving into the study presented in this chapter, a recap on the security of m-learning components and threats to m-learning system are described below.

5.2 *Threats to m-learning systems*

The variety of serious threats and various forms of attacks that affect m-learning systems are happening mainly due to vulnerabilities that remain in the m-learning development process. A typical m-learning system comprises server computer systems (application and database), web services, network infrastructure, and client

mobile devices. While servers and network infrastructure have some inbuilt security and are usually owned by educational institutions or service providers, who have adequate resources to ensure their security, mobile devices are owned by individual students and generally do not come with protective software such as antivirus. Lack of security tools makes mobile devices vulnerable to many threats and attacks. The keen adoption of m-learning by higher education institutions on a global scale because of widespread use of mobile devices requires proper security considerations in order not to expose m-learning systems to cyber-attack. Given their high portability and mobility, mobile learning devices such as smartphones and tablets are very susceptible to physical and digital attacks, and they are becoming easy targets for hackers mainly because of their widespread use (Guo *et al.*, 2013).

Digital cyber-attacks on mobile devices will continue to flourish because they are cheaper and less risky than physical attacks as hackers and cyber criminals only require a computer and an internet connection to strike, in addition to the fact that the attackers are unrestrained by distance or geographical location and they are difficult to identify and prosecute due to the anonymous nature of the worldwide web and the Internet (Jang-Jaccard and Nepal, 2014). A recent security report written by Nachenberg (2011) reveals a rapid increase in the number of mobile device attacks which is expected to continue to rise significantly in the coming years (Geier, 2012). Thus, numerous threats are waiting to attack m-learners as the Internet proliferates with hackers and attackers. Lost or stolen devices form a class of physical threat that is common to mobile devices. The mobile device is vulnerable not only that it can be stolen and re-sold, but more importantly that it may contain sensitive personal information. A survey on mobile device users showed that one out of every three mobile device users has lost their device at some point in time (Juniper Networks, 2011).

Servers and network infrastructures can also be subjected to physical and digital attacks if not properly secured (Dimkov *et al.*, 2011). Depending on the point of

entry the threats that affect m-learning systems can be categorised into application-based, web-based, network-based and physical threats (Lookout, 2013). An application-based or mobile app threat is downloadable software that may pose security issues for mobile devices. Although a malicious mobile app may look genuine, it is purposely developed to attack, destroy, disable or commit fraudulent acts. Similarly, a good native app may have flaws in design or configuration which are then exploited, attacked or hacked for malicious reasons, and malware and spyware fall into this category of threats. A web-based threat is due to connectivity to the Internet and accessing deceptive or fraudulent websites using a mobile web app or mobile browser. Web-based threats include phishing, drive-by downloads and browser exploits. Most mobile devices normally support mobile networks as well as local wireless networks such as Wi-Fi and Bluetooth. These types of networks are vulnerable to network threats such as Wi-Fi sniffing and network exploits.

The physical threats that affect servers and network infrastructures include physical damage to servers, routers, switches, cabling plant or even base stations. These often happen during student riots in some universities in Nigeria, thus leading to unscheduled downtime or denial of service. Internet connected servers in m-learning are also open to several threats and attacks that hackers are likely to use to either gain access or bring the servers down. These attacks include brute force attack, open relay, cross-site scripting, SQL Injection, and DoS/DDoS. Blended threats which involve a combination of attacks against different vulnerabilities may propagate into the m-learning systems, although an attacker only needs one vulnerable point of attack to succeed (Leung *et al.*, 2007). Therefore, m-learning systems must have comprehensive security measures in place by closing off all possible avenues of attack. Having identified a number of threats to m-learning systems, research has been conducted to investigate the following questions in universities in Nigeria.

5.3 *Experimental Research Questions*

In order to find solutions underlying research problems mentioned above, the following questions were formulated.

RQ 5.1 Which component of m-learning system is commonly attacked (mobile devices, servers or network devices)?

RQ 5.2 How is the security of m-learning devices breached in Nigerian universities?

5.4 *Design of the study*

The user-centred methodological approach discussed in chapters three and four was employed in this study. All the participants in the initial study in chapter four were the same participants for this study, thus the students and the teachers are the focused participants, since they are the main users.

5.4.1 *Data Analysis*

The data that are analysed in this chapter are based on the survey data collected through a quantitative instrument of questionnaires and some qualitative data collected through semi-structured interviews. In the results and discussions sections, the findings from the questionnaire analysis were supported with findings from the qualitative analysis. The data was also analysed using the themes to help the author to establish patterns and answer the research question answered in this chapter. The themes from the interview were extracted in Nvivo statistical package order to be statistically relevant and analysed. All the copies of the questionnaire that were administered and returned were processed and analysed using relevant statistical tools. Some statistical tests were also performed through the use of relevant models while the results are presented using descriptive statistics, tables and graphs.

5.5 Results and findings

The findings of this work are organised into three sections in order to provide answers to the survey questions as shown below.

Which component of an m-learning system is commonly attacked?

This research question relates to questionnaire number 20 and interview question 8. Figure 5.1 illustrates the opinions of the respondents regarding the common attacked components of m-learning systems. The analysis on this section of the study shows that threats and attacks are more predominant on the mobile than other devices as indicated by the students and educators.

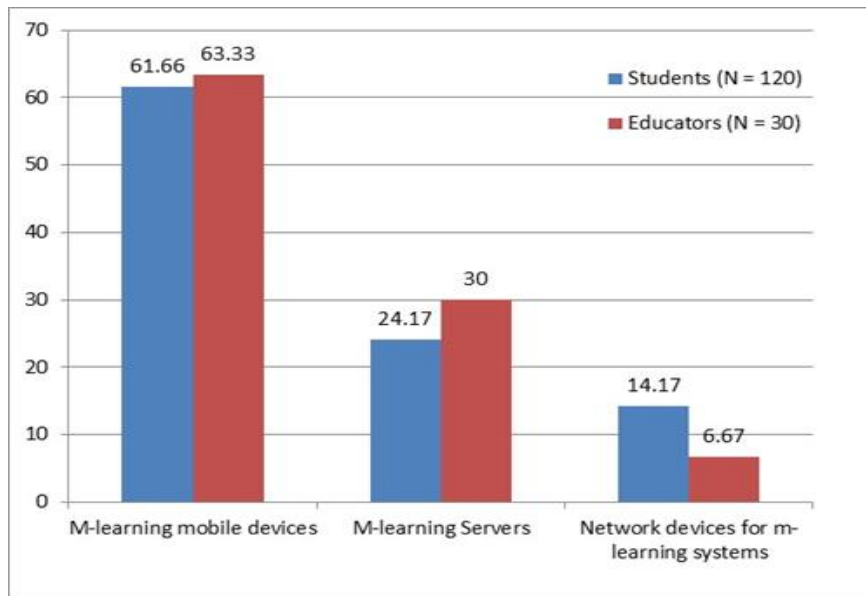


Figure 5.1: Which component of m-learning is commonly attacked?

Over six in ten, (63.33%) of the educators and 61.66% of the students responded that mobile devices are easily attacked. Server systems are next as indicated by one in ten (30%) of the educators and a quarter (24.17%) of the students. Network devices are

believed to be least attacked as revealed by only 6.67% of the educators and 14.17% of the students respectively.

How is the security of m-learning devices breached in Nigerian universities?

This research question relates to questionnaire number 13 and interview question 8 and it is a follow up to the research question above. It aims to establish how m-learning devices are breached and two questions were used from the questionnaire. The first is to determine if the security of the participants' device has been breached before. 81 out of the 120 students (67.5%) noted that the security of their mobile device has been breached or compromised before while 39 respondents representing 32.5% said their security of their device had never been breached.

The second question is to investigate how the security was breached. Figure 5.2 illustrates the responses from the participants and indicates one or more ways the security of the respondents' devices was breached. The following are notable.

- 1- 65.43% of the students indicated that they have no password lock on their mobile devices, even though this is the simplest form of security expected from the users.
- 2- Bluetooth connectivity, and the failure to disconnect Bluetooth when the connection is no longer required by the students leading to security attacks as indicated by nearly seven in ten (69.14%) of them.
- 3- Attacks through mobile browsers accounted for 64.2% on how m-learning systems were breached.
- 4- Malicious attachments to SMS or emails and downloads from unknown sources or websites have significant percentages on how security of mobile devices are breached or compromised as shown in figure 5.2.

The educators' views were also obtained through interviews to determine how m-learning devices can be breached. More than half of the educators (53.55%) indicated

no password lock on mobile devices had led to security breaches, this practice they believe is quite common among learners. Two thirds of the educators (66.67%) responded that ‘Bluetooth connectivity and the failure to disconnect the Bluetooth when the connection is no longer required by the students is a security risk. Based on educators’ opinions, attacks through mobile browsers or visiting untrusted sites accounted for 56.67% of the security breaches while malicious attachments to SMS or emails and downloads from unknown sources or websites have 63.33% and 46.67% respectively.

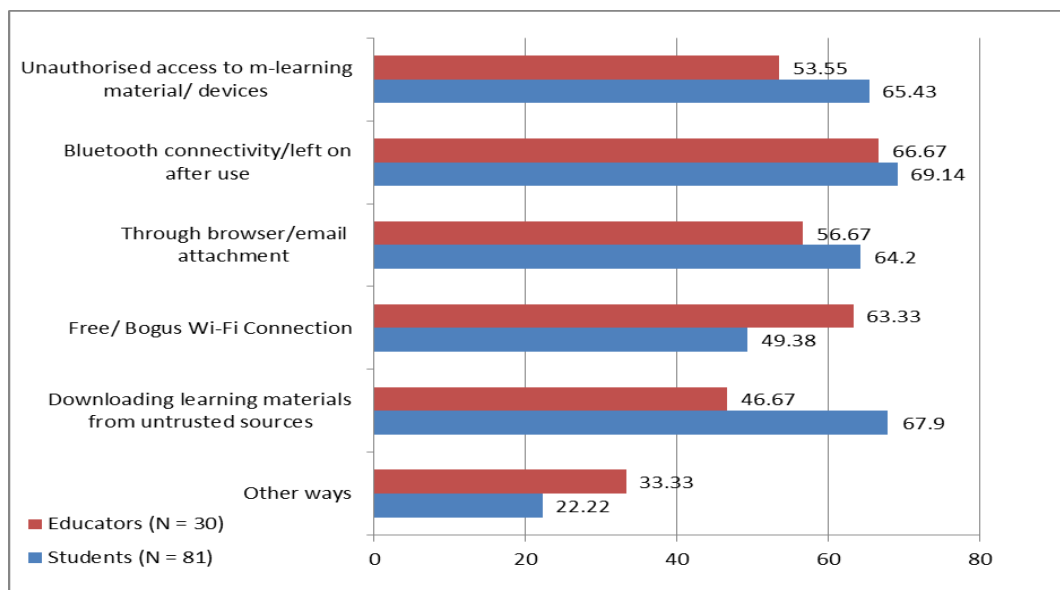


Figure 5.2: How is the security of m-learning devices breached?

5.6 Discussion

The aim of the research activities in the chapter is to identify the attack routes in m-learning in **HEIs in Nigerian context**. The findings of this investigation, together with hypotheses tested in section 5.7, have enabled the researcher to succeed in this aim. Figure 5.1 shows that mobile devices have higher numbers of security threats and attacks than the servers and network infrastructure combined. These high numbers recorded by mobile devices may be due to a couple of reasons. **Some of the**

reasons given for mobile devices been commonly attacked is due to unethical activities being perpetrated by the students among themselves. During the interview, some participants stated that ‘mobile devices are most prone to attack because it is used by students to share materials among themselves and such material may come from dubious people who wants to obtain personal information about users’.

According to Stamford (2014) an estimated two billion smartphones and other mobile devices will be shipped before the end of 2014 for general use including formal and informal education. Guo *et al.* (2013) established that recently, the total numbers of smartphones and tablets has passed the numbers of PCs and notebooks. Thus, as more mobile devices are produced, more of them are likely to come under attack from vulnerabilities in the operating systems and apps (La Polla *et al.*, 2013). This suggests that the number of attacks on mobile devices is likely to increase with the number of such devices being used by students for learning purposes.

Furthermore, servers and network devices are normally manufactured to specific security standards including factory fitted security software such as firewalls, anti-virus and defenders, mobile devices generally do not come with security software. M-learning servers and network devices are owned by educational institutions or their service providers, who have adequate resources and deployed them to ensure effective security for their servers and network facilities. They sometimes mandate manufacturers to customize inbuilt security on the servers before delivery, however, mobile devices owned by individual students are rolled out to the public and are difficult to customize for each and every student. The only exception to this are mobile devices acquired by HEIs for use by their students.

Figure 5.2 reveals how the devices are breached based on students’ experiences and educators’ engagements with mobile learning **in Nigeria HEIs**. The highest percentage of the breaches (69.14%) was through Bluetooth connectivity or when the

Bluetooth service is left on after use for sharing materials. **Many computer science students in Nigerian HEIs** do not know that they have to disconnect or switch off their Bluetooth connectivity when they are through with the usage, thereby giving access to unknown connections through which malicious programs can be passed to the user's device later on. Tipton and Nozaki (2012) indicate that several design flaws exist in the Bluetooth protocol as well as its implementation which mobile malware exploit to spread. According to Clooke (2013), the first known mobile malware, Cabir, spread through Bluetooth. Although malware spreads through mobile devices communicating using Bluetooth, typically within a few meters range, the spread can be rapid across many devices if there are many collections of Bluetooth-enabled devices. Such an attack was reported during World Athletics Championship in 2005 where many people who attended the event had their devices infected with malware within a short time (Gostev, 2006).

Visiting unfamiliar websites and downloading learning materials from unknown sources most especially **among computer science students in Nigerian HEIs** can lead to serious security breach as they accounted for 67.9%. Mobile viruses spread the same way a traditional computer virus does through download of an infected file to the mobile device over the internet (Clooke, 2013). This practice includes file-sharing downloads, mobile app downloads from un-trusted sites and false update patches. In addition, when infected webpages are browsed by using a mobile device browser, the malicious code hidden in the webpage may be triggered. This malicious code may infect the mobile device and cause some damage (Shih *et al.*, 2008) and it is more common among learners than educators. While the educators and students experienced similar security breaches, a large difference is noticed on downloading learning materials from unknown sources. This may be due to the fact that **CS students in Nigeria** download learning materials more than lecturers, and some of them may download from untrusted source. This implies that while the educators are engaged in uploading learning materials to m-learning systems, students are normally

busy downloading materials from both legitimate and illegitimate sources, thereby exposing themselves to cyber-attacks.

Malware, spyware and other malicious attacks are also spreading through SMS (Short Message Service), MMS (Multi Media Service), IM (Instant Messaging) and other messaging services by attaching themselves to the message as shown in figure 5.2. This finding is supported by Faiz and Maqsood (2009) who reveal that ComWar is the second landmark mobile malware that spreads by sending itself via MMS to all contacts in the address book. Furthermore, Shih *et al.* (2008) observes that as mobile IM usage grows, new forms of attacks on mobile devices are likely to appear, such as hijacking lists of IM names and sending links to recipients directing them to malicious sites. Mobile viruses can also send fake IM messages with the malicious code attached. Many users do not bother to password protect their devices making them vulnerable to unauthorised use which accounts for 65.43% of security breaches among students. Categorised under other ways of attacks in the study are malware that infect mobile devices by exploiting vulnerabilities in Wi-Fi connectivity. Worms that spread by exploiting vulnerabilities in Wi-Fi connectivity could also infect mobile devices that are Wi-Fi capable (Mulliner, 2013). Similarly, vulnerabilities exist in the operating systems used by mobile devices. There are reported cases of vulnerabilities in the design of some mobile operating systems that have caused the mobile device to work very slow or even crash during usage (Leaviit, 2013).

5.7 Statistical and Hypothesis Testing

In the data analysis process the researcher wanted to establish some associations among the variables using statistical hypothesis testing. In this chapter three relationships were tested. First, is there any significant difference between the learners and educators' experiences of the commonly attacked component? Second, we also wanted to find out if there is any gender influence among the students who

indicated that the security of their devices has been or not been breached. Lastly, we tried to establish if there is a statistical difference on how the security of mobile devices are breached based on students and educators' engagement with mobile devices. To answer these questions, the following hypotheses were established and tested.

H1: There are significant differences between the students and the educators on the most attacked components of m-learning system

H2: There is gender influence on the students who indicated that the security of their device has been or have not been breached before.

H3: There are significant differences between the students and the educators on how the security of mobile devices are breached.

The first hypothesis was tested using the chi square statistical test for dependency to compare the views of the students and educators on the most attacked components.

Table 5.1: What is the common attack route in m-learning system?

| The common attack route in m-learning system | | | | |
|---|-------------------|-------------------|-------------------|-------------------|
| | Mobile Device | Servers | Network Devices | Row Totals |
| Students | 74 (74.40) [0.00] | 29 (30.40) [0.06] | 17 (15.20) [0.21] | 120 |
| Educators | 19 (18.60) [0.01] | 9 (7.60) [0.26] | 2 (3.80) [0.85] | 30 |
| Column Totals | 93 | 38 | 19 | 150 |

From the table 5.1 above, the chi-square statistic is calculated as 1.3989, the P-Value is 0.496856 at the confidence interval of 0.050. The test shows that there is no significant difference between the students' and academics' views on the component of m-learning systems that is prone to attack. The test confirms that the opinions of the educators and students are the same on the route attack on m-learning systems components even though different methods (quantitative and qualitative) are used to obtain the data. The second hypothesis focuses on the gender influence on the

students who indicated that the security of their device has been or not been breached before.

Table 5.2: Has the security of your device been breached before?

| Has the security of your device been breached before? | | | |
|---|-------------------|-------------------|------------|
| | Breached | Not Breached | Row Totals |
| Female | 46 (42.52) [0.28] | 17 (20.48) [0.59] | 63 |
| Male | 35 (38.48) [0.31] | 22 (18.52) [0.65] | 57 |
| Totals | 81 | 39 | 120 |

From the table 5.2 above, the chi-square statistic is calculated as 1.8395, the P-Value is 0.75015 at the confidence interval of 0.050. The test shows that there is no gender influence between the female and male students who indicated that the security of their device have been or not been breached before. Thus, the test confirms that gender is likely to have no basis on m-learning security breaches.

On the third hypothesis, a statistical test for observable differences linked to the students and educators on how the security of their mobile devices was breached was carried out using nonparametric Mann-Whitney U Test. Table 5.3 and 5.4 below show the statistical calculations. According to the table 4, there is significant difference on the security breach experienced by the students and educators. This implies that the students and educators experience different security breaches.

Table 5.3: Ranking of students and educators on security breach

| Dimension | Participants | mean of ranks | sum of ranks |
|-----------|--------------|---------------|--------------|
| Students | 81 | 9.17 | 55 |
| Educators | 30 | 3.83 | 23 |
| Total | 111 | 6.5 | 78 |

Table 5.4: Mann- Whitney test on how the security of mobile devices are breached

| Test | How the mobile security was breached |
|-----------------------|--------------------------------------|
| U Mann - Whitney | 2 |
| Z | 2.482 |
| Asump. Sig (2-tailed) | 0.01314 |

5.7 Limitations

During the initial study including the questionnaire survey and interviews, there have been some of limitations which constrained the activities and those that particularly related to this chapter are as follows.

- 1- While the participants were asked to answer the questionnaires from experience they have had on m-learning system, some students might have answered the questionnaires partly based on their theoretical knowledge rather than security issues they experienced individually when using their mobile devices supposes.
- 2- Responses of the participants and respondents most especially during interview may be limited to their knowledge of the subject matter and their mood at the time. Therefore, the answers given by the participants may not reflective the reality on ground on m-learning security.

Nevertheless, the researcher has attempted to minimize the impact of this limitations through comparison of the methods of data collection and the results obtained from this study are accurate and consistent with related studies conducted in the field of m-learning in other parts of the world.

5.8 Summary

Having highlighted the components of mobile learning and identified that the mobile device is the predominantly attacked component and discussed how the security of

mobile learning systems are breached, the challenge is to ensure that learning systems are secured, right from the mobile devices, to the servers and network infrastructure. Since servers and network devices used for m-learning are usually owned and managed by Higher Educational Institutions or service providers, they have enough resources to engage the service of security experts to protect these two components by deploying proper security policies.

The security aspect of m-learning is often ignored when mobile devices are used for educational purposes. However, m-learning devices are prone to security threats or attacks and the user's confidentiality, integrity and data availability are at stake (Yap and Ewe, 2005). The purpose of this chapter is to spot the predominantly attacked components of m-learning, understand how the security is breached and reduce the occurrence of the attacks. Following a research study, mobile device component of an m-learning system was identified as the easiest attacked component while file sharing through Bluetooth and downloading of learning materials and content from unreliable sources are the main attack routes in Nigerian universities.

A failure in any component of m-learning environment will lead to failure for the entire system, a highly secure mobile learning environment is supposed to detect and deter threats and attack as well as having no known vulnerability weak points and being unsusceptible to failure.

CHAPTER VI

M-learning Security Framework

6.1 Introduction

In the previous chapter, we identified that the mobile device client is the main source of security breaches in m-learning environment through surveying user experience or engagement with m-learning. We also identified from our research results in chapter four that there is no suitable m-learning security framework which can be used as a foundation for developing m-learning systems, particularly in HEIs in Nigeria. Thus, the first intervention of this research is to develop an m-learning security framework for Nigerian University environments. This chapter therefore, discusses a proposed security framework for mobile learning applications which is the bedrock for designing and implementing a highly secured application for mobile devices.

During the initial literature review of this research, it was discovered that there are just a couple of m-learning security frameworks, though many frameworks can be found on m-learning platforms. Among the few found on m-learning security, only the one developed by Ramjan (2010) is a theoretical framework for mobile learning security for a Thailand university, which is not suitable for a Nigerian University. Thus, the proposed m-learning security framework was developed from the initial survey conducted during in the research survey in Nigerian HEIs and from various reviews including literature and journals with adequate consideration for established principles and models such as **technology acceptance model (TAM)** and Generally Accepted System Security Principles (GASSP) (Caroll, 2014; Merkow and Breithaupt, 2014). This chapter provides solution to RQ 3 in chapter one on how the m-learning security issues in Nigerian HEIs can be reduced through the development of security frameworks.

Since the security of information is achieved through the preservation of appropriate confidentiality, integrity, and availability (CIA), therefore, the proposed framework, which is based on the CIA dimensions, is a generic one that has the capability to identify possible threats and attacks on m-learning systems, which normally penetrate from one or more vulnerable points. The vulnerability points, which are also the sub-levels of the framework, are client, server and network infrastructure are established by analysing various kinds of issues relating to m-learning systems such as illegal access to data, unauthorised penetration into the university network and using m-learning resources by unauthorised persons pretending to be real learners and lecturers in the university, device and network corruption, device theft or loss causing attacks on the m-learning system from malicious software in mobile applications or students' devices, lecturers and the m-learning network equipment. The security framework also proposes solutions to security threats during or after the development of mobile learning systems and are able to capture threats and prevent attacks that are unique to each attack route. Thus, this chapter provides answers to RQ 3 in chapter one on how the m-learning security issues and threats can be assessed and reduced in Nigerian HEIs by providing suitable frameworks for m-learning. Before going into a detailed description of the proposed m-learning security framework, it is necessary to discuss and evaluate the existing frameworks on m-learning systems and security, in order to understand the concept on which the proposed framework was based and developed.

6.2 *Evaluating Existing Frameworks*

Conceptual frameworks for m-learning design and evaluation ranging from complex multi-level models to smaller frameworks have been proposed in the literature, the general themes among them being portability of m-learning devices, learners' mobility and interaction, and control (Kearney *et al.*, 2012) These mobile learning frameworks provide the design requirements for developing m-learning applications that can be used to support classroom or distance learning. There are notable works

on mobile learning and a few on security frameworks, some of which are examined below. Churchill *et al.* (2016) propose a conceptual design requirement for an m-learning framework design based on four perspectives namely: Resources, Activity, Support and Evaluation (RASE). The activity component is the most important which requires students to engage with intellectual and knowledge-based developments. According to the authors, the m-learning framework design should detail the entire process from the environmental considerations in which it will operate to the actual m-learning activities. The environment considerations basically involve close examination of mobility, user interface, use of high quality multimedia, and communication support. Nordin *et al.* (2010) propose an m-learning design framework for lifelong learning, based on four elements which are: theories of learning, generic mobile environments, mobile learning contexts, and learning experiences and objectives. However, it can be argued that designing content for e-learning differs from designing content for mobile learning due to many physical and hardware factors such as screen size. Another notable m-learning framework was proposed by Mohammad *et al.* (2007) based on their view that m-learning is an extension of e-learning. Their framework involves adapting e-learning materials for use in mobile devices. They stated that, in doing so, some key dimensions have to be addressed and adapted. They identified the key dimensions to be learning contexts, users, mobile device and connectivity. Their study further analysed the context in which m-learning will be used, the users and their characteristics, as well as learning strategies. Their study covered the technical aspects of the environment in which the m-learning will operate such as cost, connectivity and speed. They also considered the mobile devices and their operating system platforms on which the devices function. Another similar framework for mobile learning for an education system built on three main elements was developed by Mostakhdemin-Hosseini and Mustajärvi (2003), and indicates that mobile learning is also an extension to and future for e-learning education. The authors' framework identifies existing e-learning platforms, wireless access point technology and mobile usability as the three key elements of the m-learning framework. Mobile usability involves determining the

services of a mobile device that are used in the m-learning system. It includes the type and features of the mobile device, the mobile content design and the nature of the services. In developing a mobile learning system, wireless network infrastructures, speed, capacity and cost of services should be considered (Udanor and Nwodoh, 2010). From the article, it is noted that the existing e-learning system will influence the m-learning system being developed, but m-learning systems which are adaptive to the users and mobile devices are more complex than the typical e-learning technologies. Instructors and learners will also influence the selection of e-learning types and distribution of services to the mobile devices.

Figueredo and Villamizar, (2015) proposes a framework that consists of six phases namely: (i) Recognition, (ii) Analysis, (iii) Identification, (iv) Bases, (v) Design, and (vi) Implementation. All of the six stages have been considered as part of a process to be followed by the instructor in order to build an operational mobile integration and this process aims to respond to their learning context needs. The first Recognition stage suggests that m-learning framework should support or mediate suitable mobile devices. The Analysis stages proposes that tutor should consider the learners' learning benefits of including mobile learning in their teaching practice. Identification phase recommends that the educator must decide if including mobile learning will be done for supporting a moral strategy already designed, or if he is about to propose a new educational experience. The next stage suggests that the tutor can follow two different paths based on the decisions made at the earlier stage. The design stage proposes the instructor to design, at this point, the mobile learning strategy while the last implementation stage proposes the tutor, before implementing the m learning strategy, must decide what are the educational resources demanded by the strategy. Many other researchers state that m-learning is a mixture of mobile hand held gadgets and e-learning and they are of the understanding that mobile learning is an integral path of e-learning in order to enable students to study either inside or outside their lecture rooms (Figueredo and Villamizar, 2015). However, Sharples *et al.* (2013) argued that because of the uniqueness of m-learning, an e-learning framework cannot

be used as a mobile learning framework. However, the benefits and limitations of mobile devices have to be noted and addressed accordingly in designing m-learning frameworks and learning materials. In addition, the adaptation of existing e-learning frameworks and materials for use in m-learning platforms is a challenge (Berge and Muilenburg, 2013). Osang *et al.* (2013) also argued that mobile learning is not a mere extension of e-learning, but moderately a different learning paradigm or approach. The authors stated that this is obvious when considering the way mobile devices are used in relation to desktop or even laptop machines for learning purposes, and that the differences between e-learning and mobile learning are quite different that entire different paths are followed toward information presentation or outlook, graphics and instructional design and user experience (Kambourakis, 2013). Obodoeze *et al.* (2013) discuss a mobile security framework for Nigeria. Their proposed framework is based on the security triad of safety, attack and privacy. It also covers the physical, data and operational safety of mobile telecommunication infrastructure. The authors propose five security frameworks for implementation by mobile companies which cannot be easily adapted for mobile learning environments. Ramjan (2010) develops a theoretical framework of m-learning security for a Thailand university in a hierarchical form with threats and problems at the top, followed by vulnerability points, technological solutions, CIA dimension, ISO/IEC27001 as well as ISO/IEC17799:2005 standards and m-learning systems. However, his work was developed mainly for a Thailand University and would probably not be suitable for most African university environments.

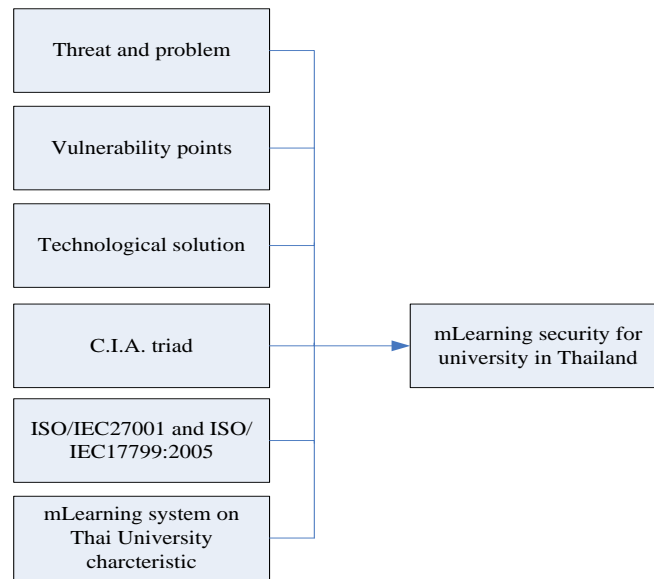


Figure 6.1 Ramjan's mLearning security conceptual framework (Ramjan, 2010)

The author indicated that their work is a theoretical framework for mobile learning security of a Thailand university. They suggest a theoretical possibility concerning threats and problems that affect vulnerability points, and give a technical solution based on C.I.A. dimension and ISO/IEC27001 as well as ISO/IEC17799:2005 standards. This thesis adopted some of the features of Ramjan's mobile learning security conceptual framework in designing and developing the proposed m-learning security framework for Nigerian university environments.

6.3 *General requirements for the security framework*

M-learning systems need effective security technologies to ensure adequate protection from different system attacks and threats. A threat is anything that has potential to cause serious harm by disrupting the operation, running, reliability, integrity and availability of a network or device and it can take any form of sabotage and can be malicious, unintentional, or an act of natural occurrence. On the other hand, an attack is an attempt used to exploit vulnerability to gain unauthorised access

to, and make use of learning materials and data, and it is aimed to destroy, expose, alter, disable, and steal m-learning confidential information. Vulnerability is an inherent weak point in the design, development, configuration or implementation of m-learning system or network that renders it liable to a threat, making it susceptible to information loss and downtime. Several researchers have noted that privacy issues remain a key concern in m-learning environments to avoid confrontation with any security threat (Kambourakis, 2013).

The basic concepts of security requirements in an m-learning system to be considered in order to cope with threats are confidentiality, authenticity, integrity, control, availability and utility, among others. Confidentiality is breached when important and personal information is disclosed to an unauthorised user within the m-learning environment and it is also an obligation to protect other learners' personal information. Confidentiality is compromised when information is breached over a network by an impostor or when a portable device with sensitive data or assessment grade is stolen or lost. This could possibly allow unauthorised person to access confidential information (Peltier, 2013; Carroll, 2014; Pieprzyk et al., 2013). Availability ensures that important learning content should be available to students when requested. Prompt access to appropriate information, material and learning content at any time is the essence of mobile learning (Kabay, 2007; Anderson, 2008). Safeguarding from attacks by keeping information protected with regards to its confidentiality and integrity is of no importance if the information is unavailable when required (Peltier, 2013; Carroll, 2014; Pieprzyk et al., 2013).

The integrity of data stored or accessed by mobile devices should be protected by ensuring that the data are correct and consistent, and that they cannot be created, altered or erased by unauthorised persons. These data should also be consistent throughout their time of usage (Peltier, 2013; Carroll, 2014; Pieprzyk et al., 2013). In the mobile technology context, data integrity also ensures that transmitted data are not intercepted, altered and modified in the process of transmission (Peltier, 2013; Carroll,

2014; Pieprzyk et al., 2013). In a mobile learning environment, integrity loss can occur, for example, when it is possible for a student to alter their grade online instead of only accessing it. Authenticity of data is the originality of content and also involves correct labelling or attribution of information which should be both genuine and original (Caroll, 2014). It is the process of verifying an identity given by or for an entity. In a mobile learning context, authenticity has two steps: identification, which is to present an identifier to the security system, and verification, which is to generate authentication information that corroborates the link between the identifier and the entity (Pieprzyk et al., 2013).

Mobile learners are normally required to pass through authentication steps in order to have access to learning materials. Control is about the physical access to the information without any need for it. If a mobile device is stolen or missing, it may results in a loss of control for the owner. However, it does not necessary imply a loss of confidentiality as access to the data may not be possible due to some security techniques such as pin lock, encryption and passwords. Data utility ensures that the data should be useful and purposeful (Peltier, 2013; Caroll, 2014; Pieprzyk et al., 2013). The data that are stored and accessed by mobile devices should be fit for purpose and if after data is secured using encryption technique and the key is lost, the data should still be confidential, authentic and available but without being useful to unauthorised users. All the general requirements are given consideration in order to develop a secure mobile learning platform. However, proper application of confidentiality, availability and integrity in designing mobile learning security encompass and absorb the functions of other requirements. Therefore, confidentiality, availability and integrity are regarded as the CIA triad dimension of security and the proposed framework presented in this paper is based on this triad of security requirements.

6.4 *Gathering and analysing the requirements*

According to the user-centred design model adopted in this thesis, stakeholders play the most vital role in the framework design procedure. In this research, the stakeholders are mainly the learners, the tutors, and some administrative staff involved in learning process. These are the contributors who enable the learning process to take place. Since the three main components in developing mobile learning technology are the student, the tutor and the learning podium, it is therefore necessary to centre the security of the learning platform in line with the experience of these users. At the beginning of the framework design some lecturers and post graduate scholars in the field of computer security were engaged by explaining to them the research objectives and indicating that this work is a contribution to research. The lecturers and learners thus set the security framework requirements based on what was to be the m-learning component to be secured, why would it be secured and how would it be secured while leaning on the Generally Accepted System Security Principle.

The requirements in this m-learning framework refer to the users' needs of a secured mobile learning platform which are presented in the research objectives in chapter one. The learners needed a secured mobile learning device which would support their learning activities, while the teachers needed a highly secured tool to support their learners without worrying about losing confidential information or privacy concerns. The contextual resources in this case were the devices that learners mostly had accesses to which were Smartphones and tablets. This meant that the development process of the system would mainly be customised for different types of mobile devices. The contextual challenges as already mentioned were: some users are concerned about losing confidential data and private information while using the portable devices for learning and teaching purposes.

6.5 *Architecture and design of the framework*

An m-learning framework normally incorporates the system architecture and design of the learning flow. It is a systemic configuration and implementation of mobile devices for learning. The m-learning system architecture is a three-layer design comprising of the (i) mobile device for m-learning, (ii) the m-learning servers (app, web and database) and (iii) the m-learning network infrastructure (El-Gamil and Badawy, 2010; El-Sofany and El-Seoud, 2009). The m-learning mobile clients consist of different varieties of mobile gadgets such as mobile phones, smartphones, netbook and tablets, and they are often programmed using different operating systems. The user interface is automatically modified to different screen sizes of the devices and connects to the servers using a Wi-Fi or WAP through a web browser. In an educational context using wireless network implementations, Wi-Fi is most commonly used when compared to other wireless (El-Gamil and Badawy, 2010; El-Sofany and El-Seoud, 2009). There is regular content update through synchronisation and the entire application is also updated when new features are added. The m-learning clients provide learning services such as viewing or accessing learning content and grades, downloading learning materials, having group discussions among learners and submitting assessments and feedback. The m-learning server comprises different servers that connect the m-learning mobile devices with database servers such as the application server and web server. While the app server consists of the web portal service that handles the direct requests from WAP or Wi-Fi and acts as an interface between the web servers, database servers and the mobile devices, the web server accepts requests for learning content from mobile clients. The database server contains the data on learners such as their login account, enrolment details, e-portfolio and assessment grades. It also holds data on the instructors as well as the learning content (Basaeed, 2009). Network infrastructure equipment ranges from switches and routers for Wireless Local Area Networks (WLAN) normally used within a university campus for transmitting and receiving radio signals and equipment for encrypting and decrypting educational data transmitted. Nowadays

mobile broadband signals are used by mobile devices for connectivity. There are public and private Wi-Fi hotspots which can also be connected to within the institution environment or household to access m-learning servers.

6.6 *The proposed framework*

6.6.1 The main framework

The proposed framework involves identifying and safeguarding possible entry points in the client, servers and network infrastructure of an m-learning system which maybe prone to attacks from cyber hackers of wireless technology devices. The hidden weak points on lecturers' and learners' devices as well as the network infrastructure need to be protected by designing a secured m-learning framework using the CIA triad dimensions: integrity, confidentiality and availability (Ramjan, 2010). The vulnerability points in an m-learning architecture - client, server and network infrastructure - can be established by reviewing various kinds of issues, attacks and threats relating to m-learning such as illegal access to data due to device theft or loss, unauthorised penetration into a university network and using m-learning resources by unauthorised persons pretending to be real learners and lecturers in university, device and network corruption causing inconvenience to users, and attacks on the m-learning system from malicious software in mobile applications or devices of students or lecturers, and on the network (Ghorbanzadeh, 2010). In order to overcome these issues, an adequate security policy to block or secure the vulnerability points of m-learning system in accordance with the CIA triad dimensions based on ISO/IEC27001 and ISO/IEC17799:2005 standards can be employed (Meehinkong, 2009). The security policy provides mobile device and network threat or risk assessment that are associated with terms of use of devices, and the structure of risk assessment and management.

Identifying and understanding the security weak points at mobile client, server and network levels are very important in overall design strategy for a secured m-learning framework (Ramjan, 2010). Once a threat or attack and its possible vulnerability points are known, providing possible solutions based on the CIA triad dimensions is feasible. Fig. 6.2 is the proposed mobile learning framework which is a generic framework having three sections: the threats and attacks, mobile learning environments and possible solutions. The mobile learning environment is subdivided into vulnerability points and the CIA triad security requirements. The vulnerability points or attack routes are the mobile clients, servers and network infrastructure described in section 6.5.1 under architecture. The triad CIA security requirements are confidentiality, integrity and availability, discussed under the general security requirement. The mobile learning framework may be used to detect any threat and deter any attack if the triad CIA security measures are properly implemented in the design and development of mobile clients, servers and the network technology of the mobile learning environment. However, if hackers are able to penetrate the learning environment using sophisticated and latest hacking techniques without being detected, a further review of the CIA security requirement should recommend a possible solution. Thus, the generic framework should detect any possible threat and attack and offer possible solutions based on the vulnerability entry point and triad CIA security measures. Threats and attacks can penetrate the mobile learning environment through the mobile device or client, the server or the network equipment as they are indicated to be the vulnerability points or attack routes into the system. A threat can spread from one vulnerability point to another and penetrate all the other mobile learning systems as the devices are connected to one another. Depending on the purpose of the attack and the inbuilt security measures, a threat can be propagated among the devices once it has entered through a vulnerability point and cause multiple damage.

In a mobile learning context, the database server may be a major target since all students' personal information, assessment, grades and feedback are centrally stored

in it while the mobile device may be a target if the purpose is to have unauthorised access to learning content downloaded in it. Similarly, once a threat penetrates successfully, it can affect one dimension of the triad CIA or all. Threats that affect integrity can also affect confidentiality or availability or both. Therefore, in tackling any threat or attack, adequate consideration should be given to the availability, integrity and confidentiality in order to achieve a meaningful and lasting solution. More importantly, utmost consideration should be directed at the triad CIA requirements at the onset during design, development, implementation and deployment of a new mobile learning environment.

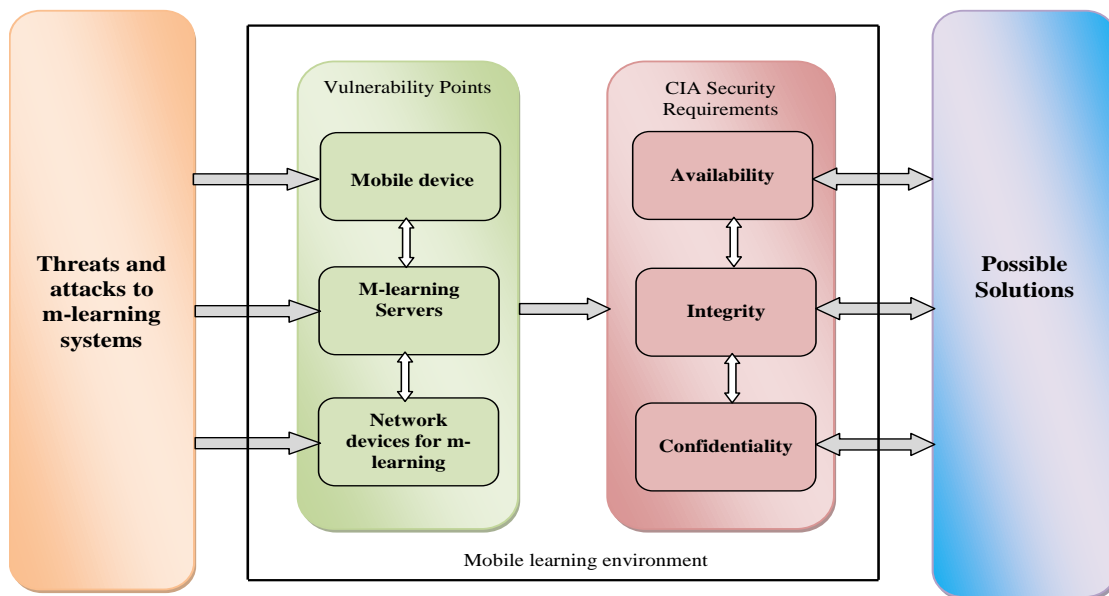


Figure 6.2- Proposed m-learning security framework

The proposed framework can be applied at each vulnerability point. The framework is subdivided into three sub-frameworks based on their vulnerability points - mobile clients, server and network infrastructure sub-framework - in order to determine threats and attacks that are peculiar to each weak point, how the triad CIA dimensions affected are handled, and possible solutions to tackle each and every threat and attack.

6.6.2 Client Sub-framework

This is a subset of the generic mobile learning framework in figure 4.2. It is designed and built to detect, prevent and give a solution to any attack or threat to portable devices being use for educational purposes. Fig. 4.3 shows the mobile client sub-framework, featuring the threat/attacks, vulnerability points, security requirements and possible solutions. The main threats or attack to mobile devices are loss/theft, malware or virus, unauthorised access and spoofing. Others such as inbuilt weakness from the manufacturers which can make hacking possible are not considered in this thesis. Starting with the threat from loss and / or theft of a device, if an individual tablet is lost for example, the CIA requirement affected is the availability as the device cannot be available for legitimate use. Regular online data backup such as the cloud backup can make another copy of data stored in the stolen device available for immediate use. The location of the mobile device can be tracked and found if lost or reported to security administrator if stolen. Remote wipe can be used for factory reset on the device to avoid confidential data being accessed by unauthorised personnel. Malicious programs attacking mobile devices affect the triad CIA security requirements. Malware or virus attack can affect availability, integrity and confidentiality of the data stored in the portable device, causing unauthorised access to learning contents or denial of service. Unauthorised access which is quite common among learners in Nigeria HEIs may affect integrity and confidentiality of the data stored in the device.

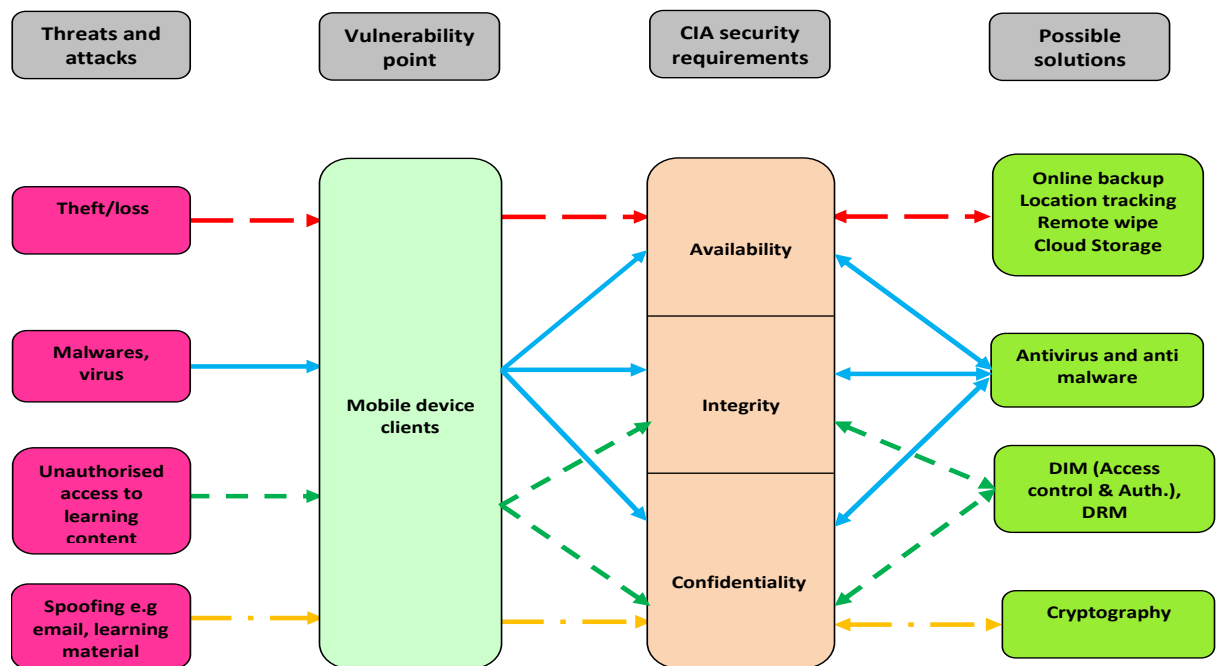


Figure 6.3 Mobile client security sub-framework

6.6.3 Server Sub-framework

The server sub-framework is designed to protect the m-learning host systems from various threats and attacks. The server system is normally situated within the university as an IT resource or as an outsourced resource and usually comprises three components or provides three services, namely web, apps and database services. Students' registration information and assessment records are saved in the database server and can be retrieved by students via their mobile services. Educational apps can be accessed and downloaded from the server by the students onto their mobile devices. Similarly, students can also access the institution's web pages through the web server from their mobile devices and download materials and instruction for studies. Thus, the security of the server sub-framework is paramount not only to the students but also to other users who engage with m-learning. The main threats to or

attacks on servers includes physical, malware or virus, unauthorised access, poor design and spoofing.

The physical attack affects availability and it is possible where there is no physical security policy in place to protect the hardware from such an attack. While a physical attack is very rare nowadays, it is still a threat in the Nigerian University environment. Physical attacks can be minimised and deterred by access control and CCTV cameras. Activities of hackers and malicious programs target poorly designed servers and affect the availability, integrity and confidentiality all at the same time. Putting in place the triad CIA requirements through regular patch updates and installing antivirus/malware can deter threats and attacks. Figure 6.4 is a server sub-framework detailing possible threats and attacks, CIA requirements and possible solutions to them.

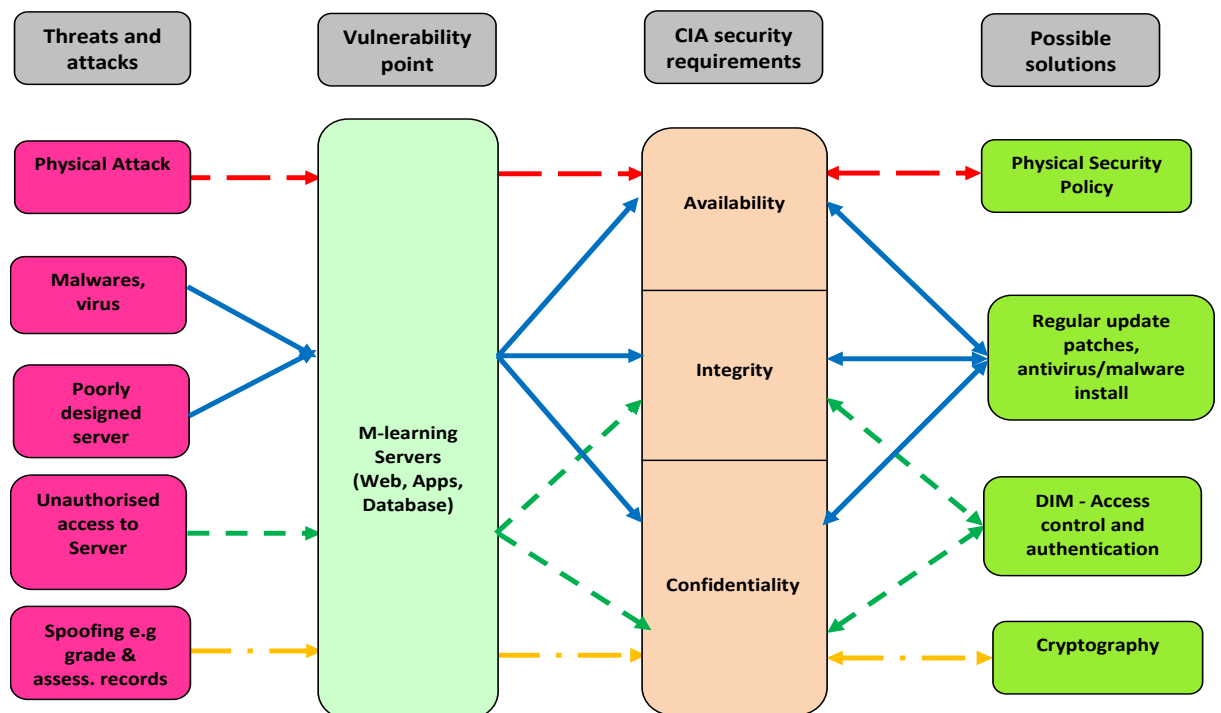


Figure 6.4: Server level security sub-framework

Similar to the client device, unauthorised access to the server by the activities of hackers may affect the integrity of the data and confidentiality of the information stored in the server. It may also affect the availability of the triad CIA if malicious activities lead to a denial of services. The threats or attack to network devices include physical, malware or virus, unauthorised access, poor design and spoofing.

6.6.4 Network Infrastructure Sub-framework

The network infrastructure sub-framework comprises of the network devices used for connection to the m-learning servers, which may range from small routers providing WI-FI services to network servers. It could also be in form of network connection provided by the mobile network service providers. The CIA requirement for network infrastructure is the need to be up and running at all time to avoid service denial. The main threats or attack to servers includes physical, unscheduled downtime, unauthorised access to m-learning network and spoofing. Aside from a physical attack that affects availability and can be prevented with adequate physical security policy, unscheduled down time/ disruption in form of power outage is a major network infrastructure threat. This is common in many developing countries where there are daily power cuts in most cities. Physical attacks on network infrastructure on campus are also common, for example during student riots in some universities Nigeria. Unscheduled downtime or disruption affects availability requirement and can be overcome by uninterruptible power supply and scheduled maintenance policy. Figure 6.5 is a network infrastructure sub-framework detailing possible threats and attacks, CIA requirements and possible solutions to them.

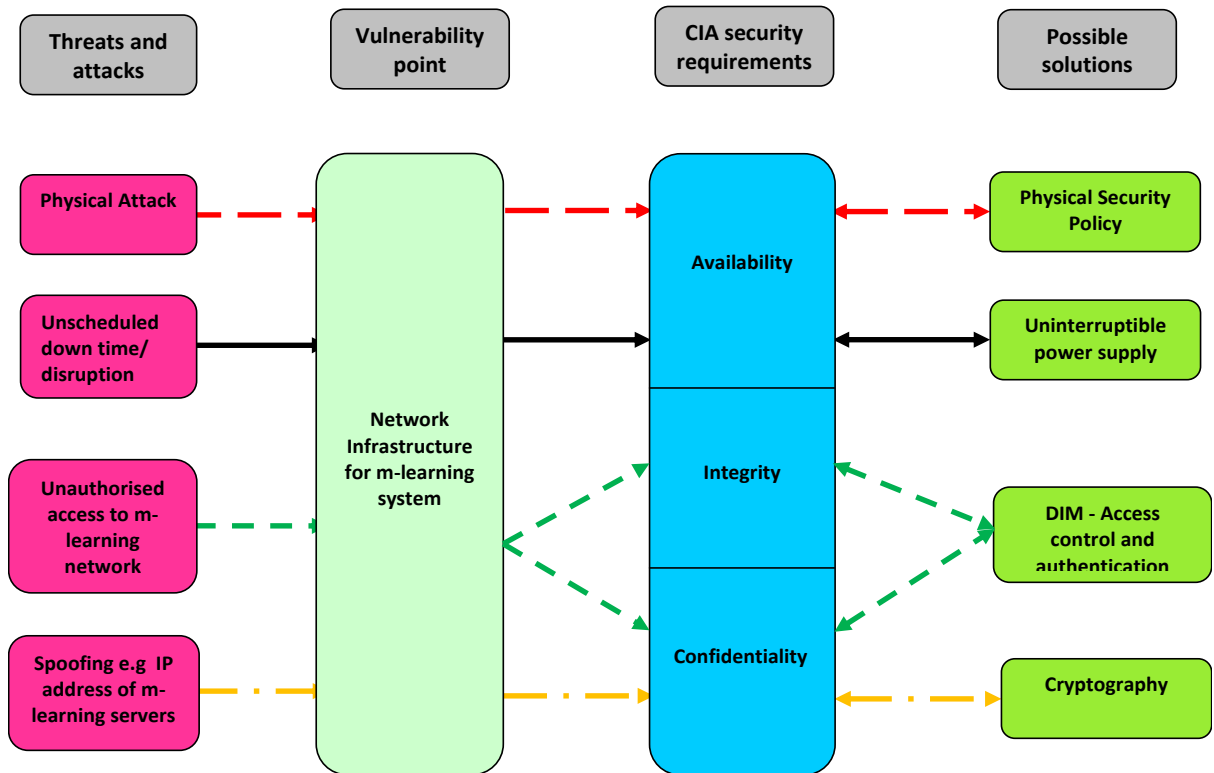


Figure 6.5: Network Infrastructure sub-frame

6.6.5 Discussion

The mobile security framework and sub-frameworks are borne out of necessity as the bedrock for designing and implementing a secured m-learning platform since there is no suitable one available most especially for Nigerian HEIs. The frameworks are extracted from literature reviews and initial survey discussion in chapter four with scholars from Nigerian using **TAM and GASSP** as guiding principles as well as ISO/IEC27001 and ISO/IEC17799:2005 standards. It can be noted that two threats affect all the frameworks, namely unauthorised access and spoofing. While unauthorised access targets integrity and confidentiality of the security dimension, spoofing affects mainly confidentiality. Access control and authentication are

possible solutions to unauthorised access while cryptography can handle threats from spoofing activities.

In order to determine if the framework and the sub-frameworks are fit for purpose and suitable as a design basis, they were further examined and evaluated during a second research survey in section 6.7 below on mobile learning security in four universities in Nigeria. The feedback from the survey shows that 11 out of 13 participants agreed that security issues around confidentiality, integrity and availability are major concerns in implementing and deploying mobile learning successfully in Nigeria education institutions. Details on the evaluation of the frameworks is described in the sections below.

6.7 *Evaluation of the Framework*

6.7.1 Aims

The m-learning security framework was developed to establish the design of m-learning security enhancement app. **This section aims to evaluate the usability and acceptability of the principle of the pedagogical design of m-learning security framework based on acceptability principles of TAM based on usability and usefulness to the users.** The evaluation was based on feedback from prospective users of the enhancement app developed using the m-learning security client sub-framework systems. The evaluation study was limited in that it was conducted as a follow up exercise to the enhancement app study, it was therefore decided that the suitable people to evaluate the framework were the teachers, learners, lecturers and post-graduate students who participated in the earlier studies in chapter four and were available at the time of the exercise.

6.7.2 Design of the evaluation method

In this study, the researcher employed qualitative data methods to conduct interviews with a total of 13 participants comprising of eight lecturers and five post graduate scholars at the University of Lagos (Unilag), Lagos State University (LASU) and Yaba College of Technology (YABATECH), Lagos. Questions for semi-structured interview was based on user-centred evaluation methodology described in chapter three, in order to determine if the frameworks were effective in supporting the security of mobile devices used in learning, thus the evaluation tackles two main objectives; the functionality and acceptability of the proposed framework in a University environment by obtaining the views of the participants on the framework. Although other methods of sampling were considered, the method that Bryman (2012) was the only method that could enable the researcher to interact with the participants in an effective manner and was therefore used accordingly. Through a voluntary process of participation, each participant was interviewed individually for about half hour.

The interviews were divided into three parts. Part one was an introduction, explaining the purpose of the interview to the participants and signing of consent form. Part two dealt with warm up questions to the main interview questions. It consisted of four questions obtaining demographic information from the participants and their background. Part three consisted of the main interview questions as follows:

- The need and usefulness of m-learning security frameworks
- Their experiences and views on the proposed frameworks
- Whether the frameworks address known issues and concerns
- The most relevant sub-framework for m-learning security
- Suggestions on improving the frameworks.

A detailed template of the framework evaluation interview questions is attached in appendix 3.

6.7.3 Analysis of the evaluation

The responses from one participant to another are similar words and meaning therefore, key words are selected and used to summarise these responses as below:

(a) The need and usefulness of m-learning security frameworks

The participants were asked about the need and usefulness of m-learning security frameworks. 9 out of the 13 participants acknowledged the need for m-learning security framework as a basis for designing security software. One participant said “Due to high security issues in the education sector and in Nigeria as a whole, I think it is necessary to have a security framework for m-learning which will serve as a guiding principle for security implementation”, another participant said that the framework is needed in order to better understand the security issues within m-learning system. However, some participant said that they are not necessarily sure of the need for the framework since there are security standards such as GASSP in place. Another participant who objected said that only m-learning system developers can determine the need for security framework. Above all there is a positive attitude towards having a robust m-learning security framework in place which will be a prerequisite for design and development of a secured m-learning system.

(b) Users’ opinions and views on our proposed frameworks

The participants were asked to give their opinions on our proposed frameworks, and we obtained different views from them. While some of the participants are of the opinion that the proposed framework is a simple security concept from the researcher, others think the framework is only theoretical and may not reflect the real security issues. Some participants also indicated that the framework is a diagrammatic representation of already known issues and looks quite familiar with existing security principles and models. A good positive response obtained is

that the security framework makes it clear to identify issues at each level of the m-learning system in a clear and precise manner, which could be developed into a standard for implementation. Thus, the overall view is that since there is no other suitable m-learning security framework in place, I think the framework will serve as a foundation which may be used for designing and developing a secure m-learning system.

(c) Framework addresses known issues and concerns

One of the main purposes of the evaluation of the framework is to determine if the framework addresses the known security issues and concerns in HEIs in Nigeria, thus the participants were asked the question during the survey. The general consensus is positive that the framework addresses necessary and common security issues. However, there are couples of negative feedback received, one of which is that the framework only addresses common issues, there are still some others not address by the framework. Another negative feedback is that the issues listed in the framework cannot be tackled without proper coding and it does not address soft issues like lack of awareness. Above all, the security concerns addressed in the framework is adequate and reflect concerns in our HEIs and that the security issues addressed by the framework are the prevalent ones that need urgent attention.

(d) The most relevant sub-framework to m-learning security

This question is to determine the most relevant among the three sub-frameworks in order to focus our attention on it as well as finding a way to reduce the security issues through it. The feedback showed that 8 out of 13 participants are of the view that the mobile sub-framework is the most relevant since it appears to be the most prone to security issues because of its mobility. Some participants considered the servers are most relevant that need to be very secured as it stored more users' confidential information than any other sub-frameworks, thus making

the servers target for hackers. However, since most server systems have inbuilt security while mobile devices have little or less security in them, the view of the majority that the security of mobile sub-framework is relevant and should be given priority.

(e) Suggestions on improving the framework

Suggestions on improving the framework was obtained as part of the evaluation process from the participants. Some of the suggestion obtained should including e-copyright concerns mainly from academic writers, the possible solution for unauthorised access in mobile device client can include biometric features such as finger prints and if possible, the client sub-framework can have some security education and awareness as part of its possible solution to lower risks. Other suggestion includes making provision for some prevalent issues common to m-learning in Nigeria such as digital right management and concerns on e-assessments.

6.7.4 Discussion

The result of the analysis on the need and usefulness of m-learning security frameworks in **Nigerian education context** shows that 10 out of the 13 participants indicated that there is a requirement to have a secure framework for mobile learning systems, which is to serve as a reference point for designing, developing and implementing a secured m-learning. Their opinions and views on the frameworks are also positive as shown from the analysis even though some of the participants observed that the frameworks are just conceptual design. The results also show that the frameworks address known security issues and concerns most of which are prevalent among the students in HEIs in Nigeria. The outcome of the analysis also reveals that the client mobile device sub-framework is the most relevant framework in terms of m-learning components that need to be most secured. This is due to the

fact that threats and attacks are more predominant on the mobile client devices than on the server and network infrastructure (Shonola and Joy, 2014), and therefore, future efforts on security frameworks should be directed to having extremely secured mobile client device. The couple of suggestions have being considered in the final design of the frameworks and security enhancement app.

6.8 Summary

This chapter discusses a proposed mobile learning security framework that can be used as a foundation for designing and implementing a highly secured mobile learning environment. The framework and sub-frameworks are based on literature of good practice, ISO/IEC27001 and ISO/IEC17799:2005 standards and in particular, the mobile framework proposed by Obodoeze *et al.* (2013). However, certain adaptations have been made to the framework to make it suitable for a learning environment. While Obodoeze *et al.*'s (2013) research work was developed for telecom operators in Nigeria and their framework is based on the security triad of safety, attack and privacy, the framework proposed in this thesis is based on the confidentiality, integrity and availability dimensions and is focused on higher education institutions in Nigeria. Our proposed framework is also in line with the research done by Ramjan (2010) and El-Gamil and Badawy (2010) but provides a broader view by taking into account up to date information, modern mobile devices and the technology acceptance model in the design of the framework.

The popular user-centred evaluation was adopted as the evaluation methodology for the frameworks having taken into account **the usefulness and usability on TAM principles**. The analysis of the evaluation shows that the mobile device client sub-framework is the most relevant of three sub-frameworks.

The next chapter will focus on our intervention to security issues in m-learning by developing a security enhancement app mainly for students in HEIs in Nigeria. The app is a product of the research activities on security threats and it aims to reduce the level of security breaches among students through awareness promotion, performing security checks on some specific mobile devices and alerting users on suspicious activities of installed apps.

CHAPTER VII

M-learning Security Enhancement app

7.1 Introduction

In the last chapter we discussed the security concerns that users have experienced when using mobile devices for learning purposes. We gathered data from their experiences on various threats and analysed the data to help identify the security concerns from stakeholders' points of view. We were able to understand that there is lack of awareness and security education among students, particularly in relation to mobile device usage. Due to lack of awareness, many students do not make use of simple security measures such as password and pin locks that are already inbuilt in their devices. Also, we are able to understand that apart from inbuilt security features the alternative ways to enhance security of mobile devices are very limited. In this chapter, we present a mobile security enhancement app, designed and developed for Android smart mobile devices, in order to promote security awareness among students. The app can also identify major security weaknesses, scan or check for vulnerabilities in m-learning devices and report any security threat. This app serves as an intervention and a contribution of this research project in enhancing the m-learning devices. Thus, this chapter provides answers to RQ 3 in chapter one on how the m-learning security issues and threats can be assessed and reduced in HEIs using our proposed m-learning enhancement app. Before going into detail descriptions of the proposed m-learning security enhancement app, it is necessary to evaluate the existing m-learning systems and security.

There have been many security incidents reported when using mobile gadgets ever since these devices have become popular, most especially in open operating systems (La Polla *et al.*, 2013). With increasing use of mobile devices and applications, many users are not aware of the growing security threats in using these devices for storing or accessing personal and sensitive information and many users are also not aware

that some mobile application are unsecure as they appear to be. As more people use the smart devices for their educational and financial activities, the more attractive the gadgets become targets to attackers with mischievous or bad intentions. In the recent security survey, it was reported that there is a rapid increase in the number of mobile security risks and how sophisticated the threats were. More worrisome is that an open and popular platform such as Android provides an easy environment to exploit and propagate security attacks (Russello *et al.*, 2011).

To prevent or limit such undesirable attacks, Android developers are integrating security mechanisms and features that allow protection of users from malicious apps. Developing an effective and usable security model which is suitable for small portable devices is not an easy challenge. In fact, while addressing many security issues, the Android security model itself has many shortcomings and security is one of the main concern about using Android smartphones (Mohini *et al.*, 2013), however some of the security issues are being addressed by Android security extensions such as Yet Another Android Security Extension (Tarle, 2015).

Another issue concerning mobile device and m-learning security is lack of awareness or negligence among users as many learners do not regard security as important until an issue arises. For example, despite the fact that the most widely used methods of authentication on mobile devices are pin locks and passwords, a number of studies show that some mobile device users are unaware of, or do not bother to use, these security features. A survey of 297 mobile phone users reported by Clarke and Furnell (2005) found that 34% of the participants did not bother to secure their device with the use pin lock or password security, notwithstanding the fact that these security measures do not offer the best protection features.

Therefore, there is an urgent need to promote security awareness and education among users, most especially among the young generation who are learners in higher educational institutions. Students need to understand the security threats and possess necessary knowledge on security, when using their mobile device for learning and

other purposes (Qian *et al.*, 2012). There have been a number of efforts on promoting security education among students for smart mobile devices; however, more efforts are still required in improving this security awareness, in terms of designing and developing security enhancement apps for m-learning users to raise security awareness, scan devices for vulnerabilities and report any potential threats in their devices. The security enhancement app proposed in this chapter serves this purpose and the chapter is organised as follows: section two presents related work on m-learning security, section three considers m-learning security app design, section four discusses the implementation and app evaluation of such an app, and section five and six present the results of the evaluation, section seven gives further discussion on the results and section eight presents the conclusion.

7.2 Evaluation of existing security measures

Researchers are now focusing their attention on mobile security issues due to a sharp rise in the number of reported mobile operating systems vulnerabilities, particularly in the Android platform by publishing many work on inherent security issues in mobile devices and m-learning platforms. Polla *et al.* (2013) presented a paper on ‘a survey on security for mobile devices’. The authors review the vulnerabilities and solutions over seven years by targeting reported high level attacks on applications. The authors gathered existing methodologies at securing mobile gadgets against different kinds of attacks and categorised them on the basis of: (i) detection principles, (ii) architectures, (iii) collected information and (iv) operating systems, particularly focusing on inception detection based models and tools with the view of providing a simple and concise assessment of the fundamental model embraced by each method.

Marforio *et al.* (2013) investigated application collusion threats based on permission security model and its consequences for mobile and smart systems. The authors demonstrated a technique on how permission based mechanisms are used on mobile

platforms to allow attacks by colluding applications that communicate over explicit and covert communication channels. This is a security bug which allows applications to indirectly execute operations that those applications, based on their declared permissions, which should not be able to execute. The security threats include disclosure of user's private data (for example call contacts and addresses) to distant parties by apps that do not have direct access to the data or cannot directly establish remote connections. The authors also disclosed that on mobile devices, many users are not aware of possible implications of app collusion while they are indirectly made to consider that by approving the installation of each app independently, based on its declared permissions, the damage that an app can cause to their device will be limited. The authors revealed that this is not correct and that application permissions should be displayed to the users differently and explicitly showing the implications on installing the apps.

Shabtai et al. (2012) proposed a security framework on Hostbased Malware Detection System that monitors the features and activities of mobile devices and apply Machine Learning anomaly detection techniques to classify the data as normal or abnormal. The authors established four malicious applications which have ability to check and detect new malware based on samples of known malware on the test data. The authors later evaluated some of the anomaly detection algorithms, feature choice procedures so as to determine the combination that gives the best performance metrics in the new malware detection on android devices. **While their system appears suitable, it may require many processing power and its usability by students is doubtful.**

Although Android devices are built in a complex method, they are still vulnerable and are still attractive objects for hackers because of their wide application domain. Therefore, the need for strong protection is inevitable, preferably using multiple and diverse attack or threats detection mechanism. This chapter presents a practical mobile technology based learning approach to enhance security experience with a focus on students' needs. The approach describes the development of a mobile

security app, which covers fundamental and emerging security issues and threats in modular form. Since using smart devices is becoming an integral part of students' daily activities, this approach provides a convenient and effective way for students to enhance the security of their devices. Thus, the three main objectives of the intervention app are the following.

- 1- The security enhancement app helps students to understand not only classical in-built security models and solutions, but also problems in emerging areas in mobile security.
- 2- The app scans or checks the student's m-learning devices in order to identify possible vulnerabilities in such devices. In case some security lapses are detected in which case, it gives tips on how to resolve them.
- 3- The app presents a report on the identified security threats to the users as well as recommendations on tackling the identified issues. With these objectives in mind, the app architecture is based on our proposed security framework for mobile clients.

7.3 Requirements, Design and Functionalities

In order to understand the current security problems affecting smartphones and tablets being used for m-learning in Nigeria, we investigated threats, vulnerabilities and attacks specific to these devices and examined ways in finding solutions to them. In particular, we reviewed literature, journal publications, policy documents and carried out surveys with stakeholders in higher education institutions, focusing our attention on high-level attacks as discussed in chapter four, five and six of this thesis. Stakeholders play the most important role in the system design process. In this research, the stakeholders are the learners and the teachers and some administrative staff in relevant departments where the survey where conducted. In agreement with

this, Paolucci (2014) mentioned the three main components in developing m-learning technology as the learner, the teacher and the learning platform.

The requirements are then documented and thereafter used to develop a system based on the user requirements. **The user requirements in this research refer to the learner's needs for a secured mobile learning system in order to engage m-learning without concerns or worries.** The contextual resources in this case were the devices that learners mostly had access to, which were the smartphones and tablets. This meant that the development process of the system would mainly be customised for these devices. Having identified some issues, our intervention is to design and develop a mobile app that will enhance the security of any device that is installed on, through promoting awareness, scanning devices for vulnerabilities and reporting threats.

7.3.1 The App Objectives and Architecture

The three main objectives of the intervention app are: 1) to enable students to understand not only the standard in-built security models and solutions, but also issues in evolving regions of mobile learning security; 2) to scan or check students' m-learning devices in order to identify possible vulnerabilities in such devices, and if some security lapses are detected, to give tips on how to resolve them; and 3) to present a report on the identified security threats to the users as well as recommendations on tackling the identified issues. With these objectives in mind, the app architecture, which is based on our proposed security framework for mobile client is designed as follows.

The architecture of the app adopts an activity-list modular structure that arranges the security issues into a sequence of self-contained units; each activity-list emphasises on a specific security issue as identified during our research study and those obtained from academic publications which include lecture notes, survey questions and interviews as well as case studies. There are awareness tips on each m-learning

security issue which are based on current research findings. Following the tips comes a security scan or check facility to analyse the mobile device and its installed app for any infection and provide advice on how to deal with the issue.

The app is developed on JAVA programming language for Android platforms due to the following three motives. Firstly, the Android devices dominated the world-wide smart phone market with 82.8% as at second quarter of 2015 according to data from the International Data Corporation (IDC) in 2015 on Worldwide Quarterly Mobile Phone Tracker. Secondly, the platform is popular and open-source having less restrictive market policy which makes it a prime target for malicious applications. Lastly, the Android platform, although it has big major backers such as Samsung and Google, is very affordable in comparison to other mobile computing platforms. The architecture of the app is outlined in the system diagram in Figure 7.1 below. The diagram provides an activity-list of security issues on which awareness tips are given and vulnerability scans that can be related to each issue.

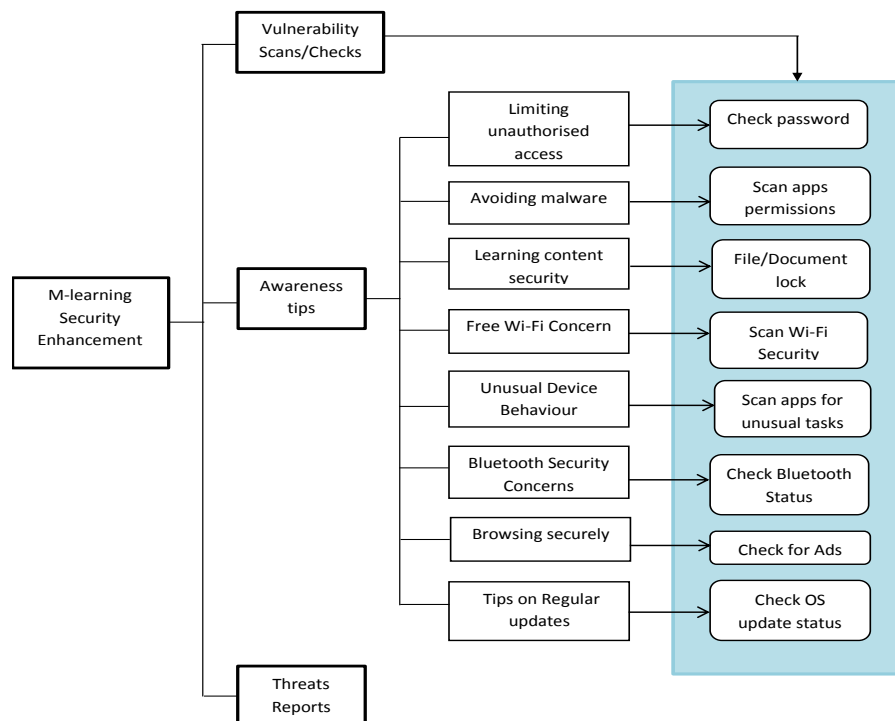


Figure 7.1: System diagram of the architecture of the app

7.3.2 App Architectural Design

As this thesis does not concentrate on the technical aspects of systems development, we used an existing software development approach based on user-centred design methodologies in designing the security enhancement app as it is important in providing support for the design and development process. Many conventional development methods have been criticised for their lack of user involvement and lack of flexibility during the systems development process as they require a stringent sequence of development. Thus, we engaged a user-centred design and development approach as this method often provides higher user involvement throughout the design process while maintaining product quality through continuous iterations with the users (Galer *et al.*, 2016). Two methods are adopted for use in the development of the security enhancement app, they are Structured Systems Analysis and Design Method (SSADM) and Rapid Application Development (RAD).

SSADM stipulates that an initial feasibility study must be performed before any system development occurs and the requirements of the system are then analysed focusing on the needs gathered from the feasibility study and on the context where the system will be used. The Rapid Application Development (RAD) is a methodology which follows a 'trial development approach'. The development of the system involves a high amount of user involvement as different prototypes of the system are developed and tested through an iterative process before a final product is achieved. The method is also best used for development of system which require consistent change to the design of the system (Konstantinou, 2013). As this method is often used in low budget product development as it requires fewer resources for small iterations of the prototype, it fits into the financial capacity of the researcher.

The development and implementation of the m-learning security enhancement app as an intervention is a main goal of this research. The design content of this app reflects users' requirements which were gathered in the initial survey study in chapter four of

this thesis. The flowchart in the Figure 7.2 below shows the basic flow of activities within the app.

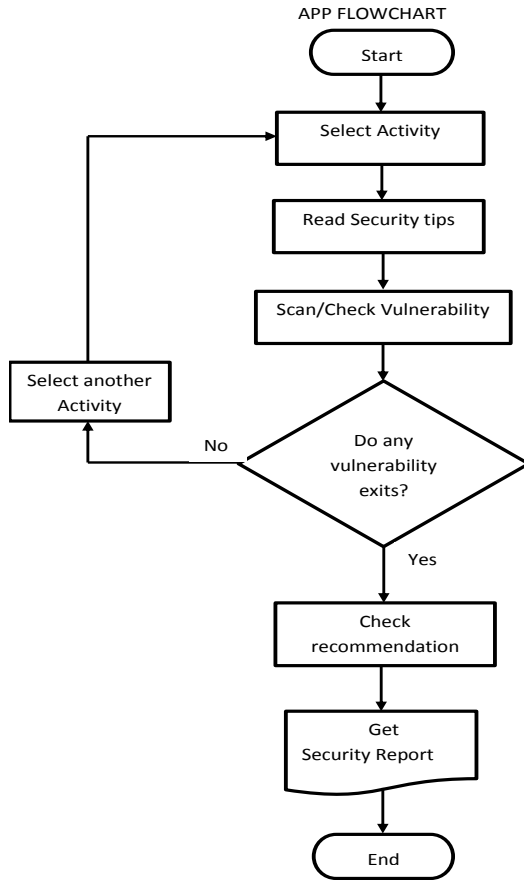


Figure 7.2: The app flowchart

7.4 App Functionalities: How it works

The app functionality and how each module or section in figure 7.1 of the app is described in this section. The screen shots for home and activity pages of the app can be seen as shown below. From the home screen (Figure 7.3), users can move to the activity-list page by clicking on the “Security tips and scans” tab.



Figure 7.3: The app home page and activity list

From the activity-list page, users can select which security activity to explore in order to read the app security tips and check or scan for vulnerabilities. The functionality of each section of the app is described below

7.4.1 Limiting unauthorised access

The first functionality of the app is ‘limiting unauthorised access’ to the m-learning device **by doing password security checks. This section checks if password security for screen lock is being used for locking the device by the user.** This is necessary because research has shown that many students do not use password lock on their device which make their device prone to threat. Many students do not have simple mobile device screen lock mechanisms such as Pattern, Pin or Password which may prevent unauthorized access to the device as well as the learning content in it. Using this app, the user will be prompted to secure their device using the security lock menu as shown in figure 7.4.

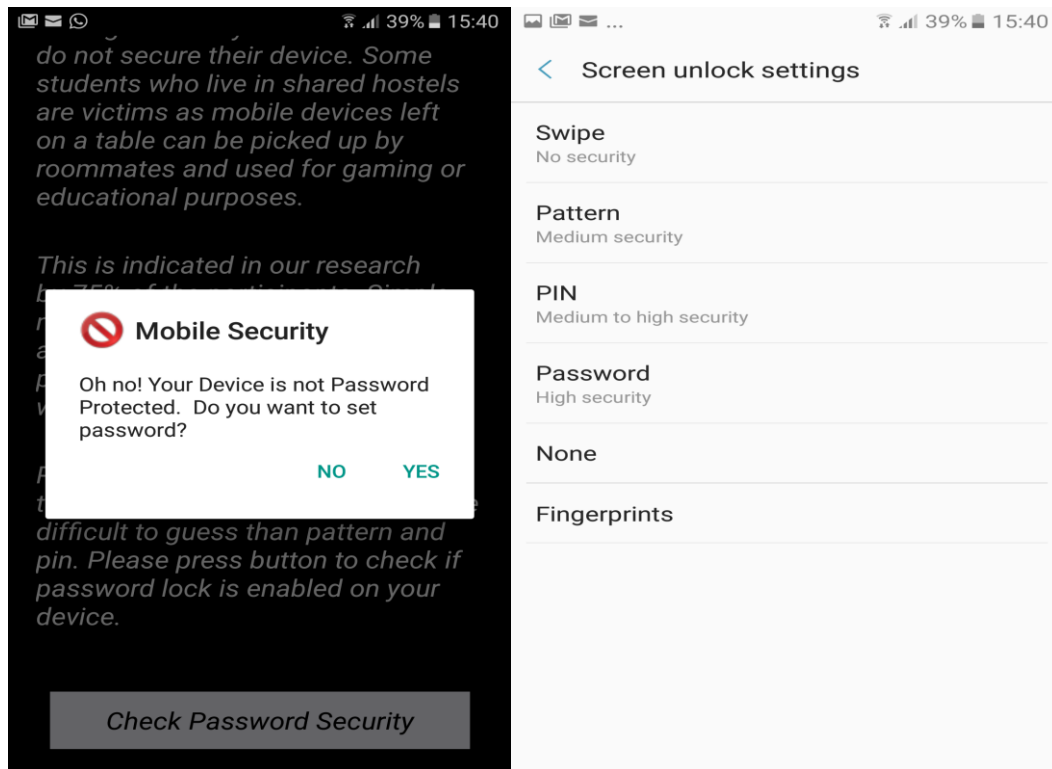


Figure 7.4: The app password security check

7.4.2 Avoiding malware attack

The second functionality of the app is 'avoiding malware attack'. **This works by monitoring permissions requested by other apps during and after installation.** Malware infection is normally caused by downloading and installing malicious app as discovered in our research study. Thus, malicious app may be avoided by paying attention to the permissions requested during installation. A list of all installed apps and their permissions can be seen through the app as shown in figure 7.5 and if suspicious permissions are noticed, users can review them or remove such app if necessary. This functionality scans for permissions granted to all installed apps and any suspicious app can be triggered for further analysis and subsequent removal if necessary.

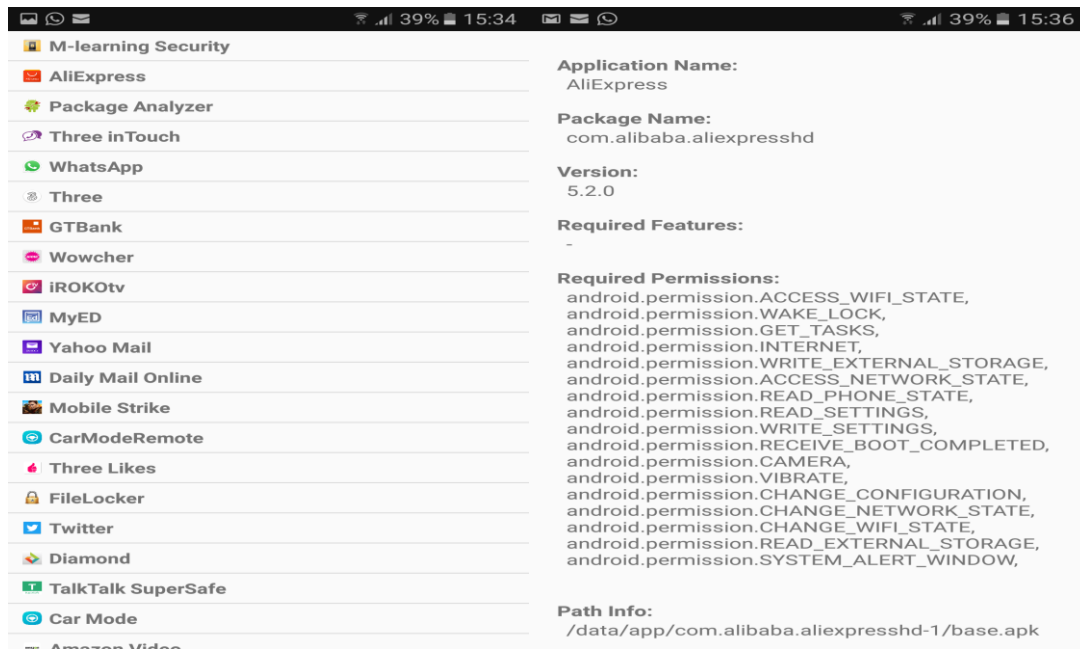


Figure 7.5: The app list and permissions

7.4.3 Learning Content Security

The next functionality of the app is 'learning content security'. **This works on user's device by using file and folder password encryption on learning documents stored on the device.** Securing learning content involves making sure that students have access to right materials and instruction to carry out their learning activities and access to materials not required for learning purposes should be denied. Since unauthorized access to learning content is a security concern, students are not allowed to view learning materials not related to their course. This ensures confidentiality and integrity of learning materials. Therefore, locking learning documents stored on mobile device as shown in figure 7.6 using file-lock password strengthened the security of their device.

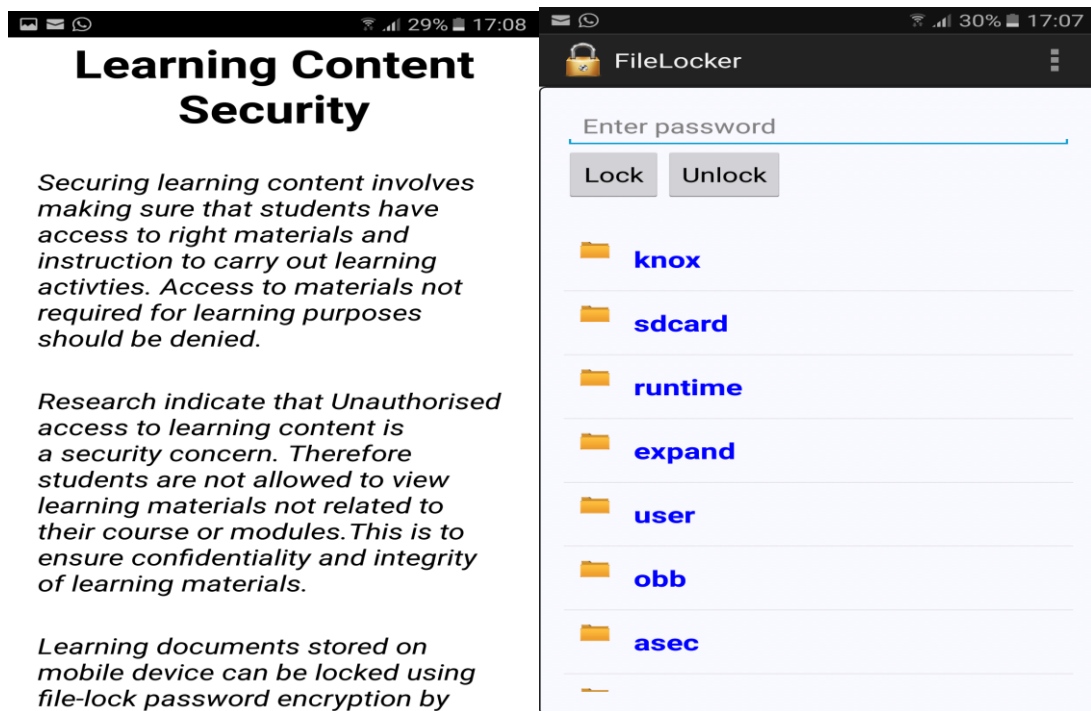


Figure 7.6: The app learning content security

7.4.4 Free Wi-Fi Concern

The functionality on 'Free Wi-Fi Concern' warns the students on the implication of connecting to free Wi-Fi provided to the public by unknown people or organization. **It also scans for the security of the Wi-Fi which the device is connected by determining if the Wi-Fi is protected by WPS, WAP or WAP2 technology as shown in figure 7.7.** Many students access educational resources online using any free Wi-Fi that is available with little regards for security of the network they are connecting through. Our research have indicated that free public Wi-Fi may not be safe as we think because they may be set up by hackers to obtain personal information from users or intercepted for malicious activities. Recent security documentary on channel 4 shows how criminals can easily suck information out of smartphones using public Wi-Fi. This risk can however be reduced by ensuring that

users are connected to a secured free Wi-Fi. The app advice students to disconnect from unprotected Wi-Fi if they had already connected to it.

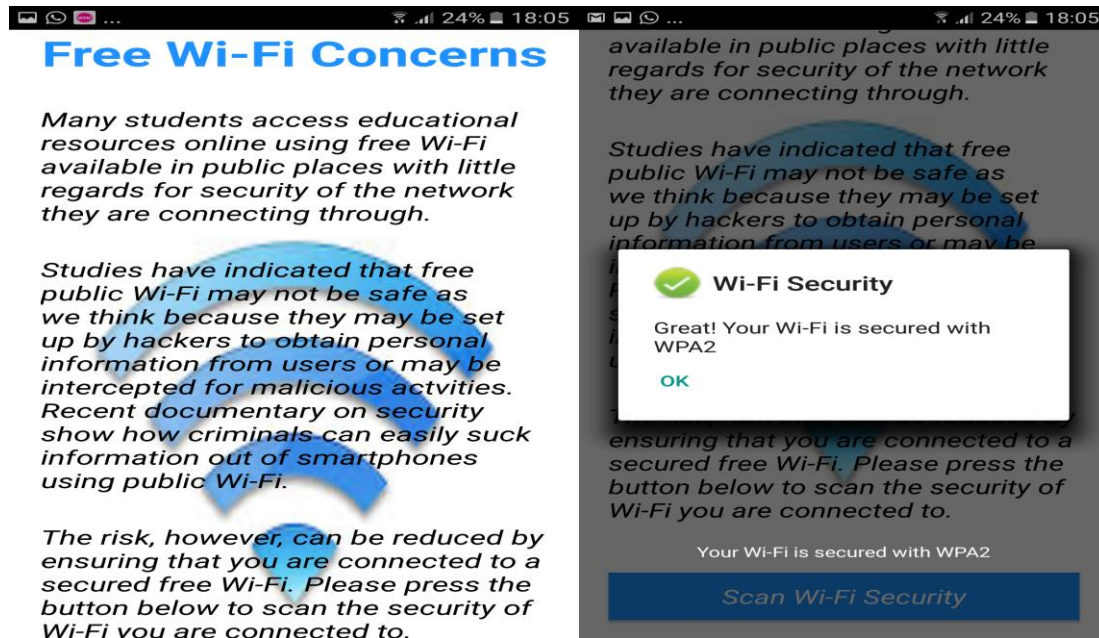


Figure 7.7: The app Wi-Fi security

7.4.5 Unusual Device Behaviour

If a user wishes to detect unusual device behaviour, they can select the “unusual device behaviour” activity and start the scanner by clicking on the service button at the top on the page (Figure 7.8). **This enables the app to start monitoring activities on all the installed apps.**

The functionality under unusual device behaviour scans the device for apps that request for high resource activities in term of memory usage, processing time and permission. Such high demanding apps are watched by the security app for ten minutes and if such requests are in use, the demanding apps are marked with ‘Red Colour’ in the app list (figure 7.9). The security app further send notifications to the user on the high resource demanding app. Apps marked with Yellow or Green Colour

are using moderate device resources. It should be noted however that high resource demanding apps are not necessarily malware or threats. The user needs to be aware of their activities and review their need on individual basis.

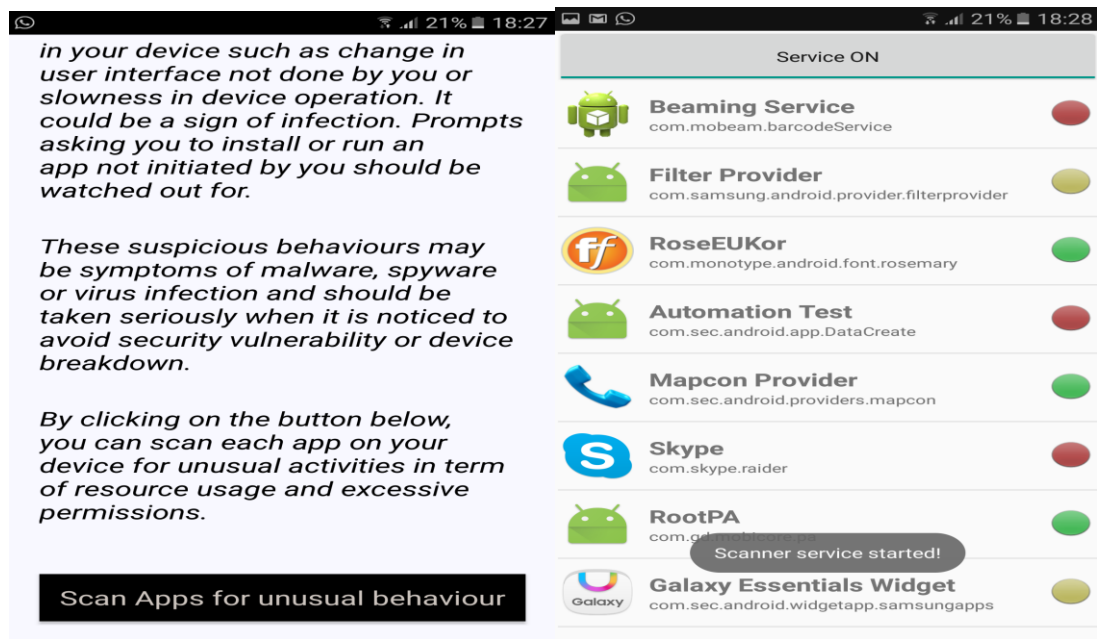


Figure 7.8: The app scanner service

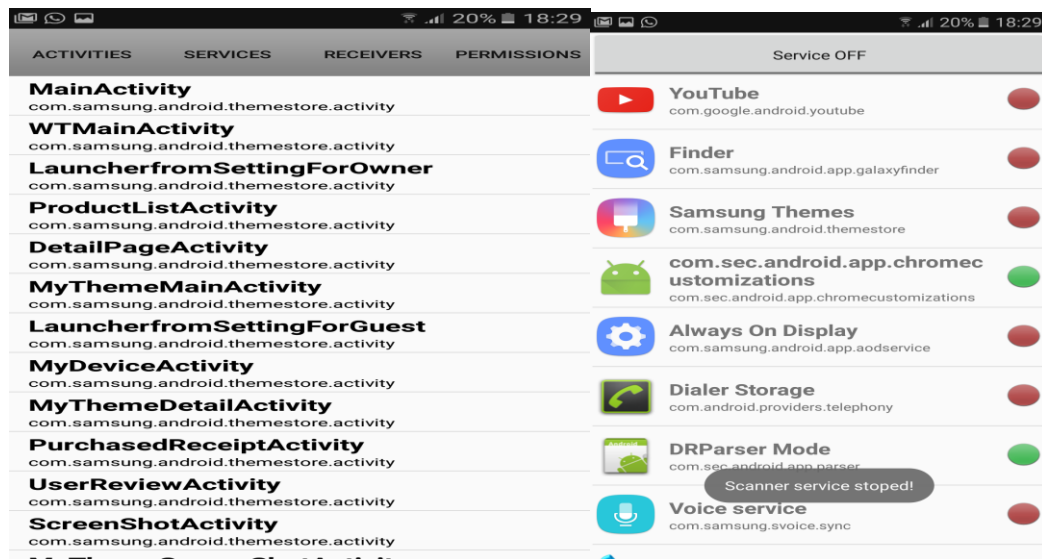


Figure 7.9: The app scanner service II

7.4.6 Bluetooth Security Concern

The 'Bluetooth Security Concern' functionality advice students on the importance of ensuring that Bluetooth connection is disabled after use. The Bluetooth Security is important as Malware and spyware spread quickly through Bluetooth connectivity. The module works by checking the Bluetooth status of the device if it is currently switched off or not as shown in figure 7.10 below.

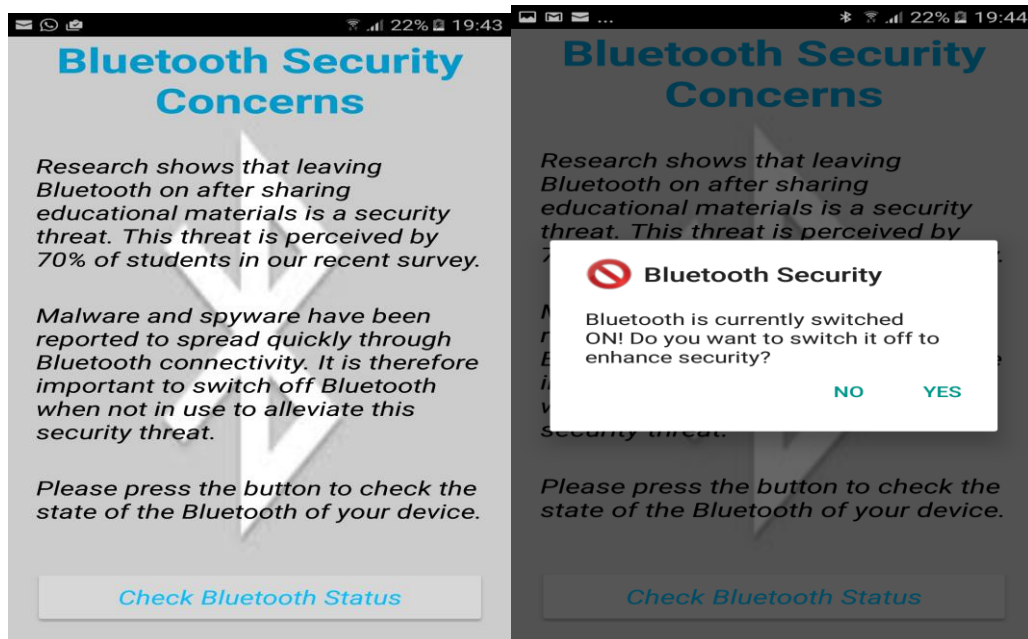


Figure 7.10: Bluetooth Security

If the Bluetooth is switched ON, the user is notified and the Bluetooth can be switched OFF from the app menu on the screen by clicking on 'YES'. Once the Bluetooth is switched OFF, the user then get a notification that 'Bluetooth is now switched OFF. Security is enhanced as shown in figure 7.11 below.

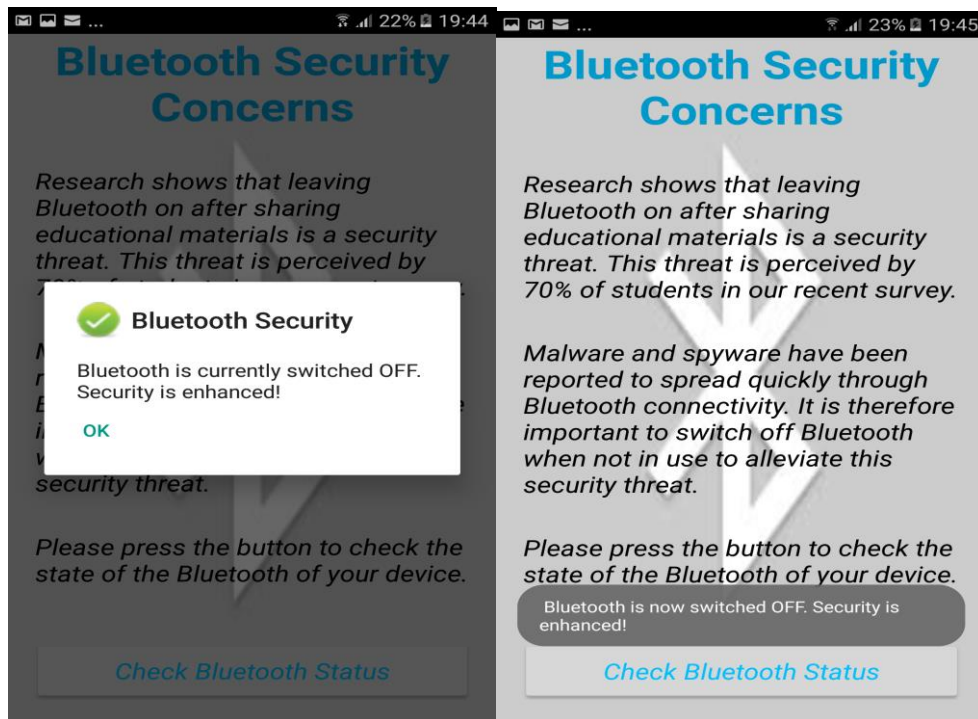


Figure 7.11: Bluetooth Security II

7.4.7 Browsing Securely

As research shows that adware, spyware and malware spread through adverts that pop up when browsing the internet or from freely downloaded apps (Le Thanh, 2013).

One method to reduce spyware and malware while browsing the internet is to block adverts that pop-up when browsing. The functionality of 'Browsing Securely' checks the device if an advert blocker is already installed, and if not, the app provides a link to download and install an advert blocker as shown below. It is up to the user to install the adverts blocker or not but our security enhancement app suggested installing it for enhanced security.

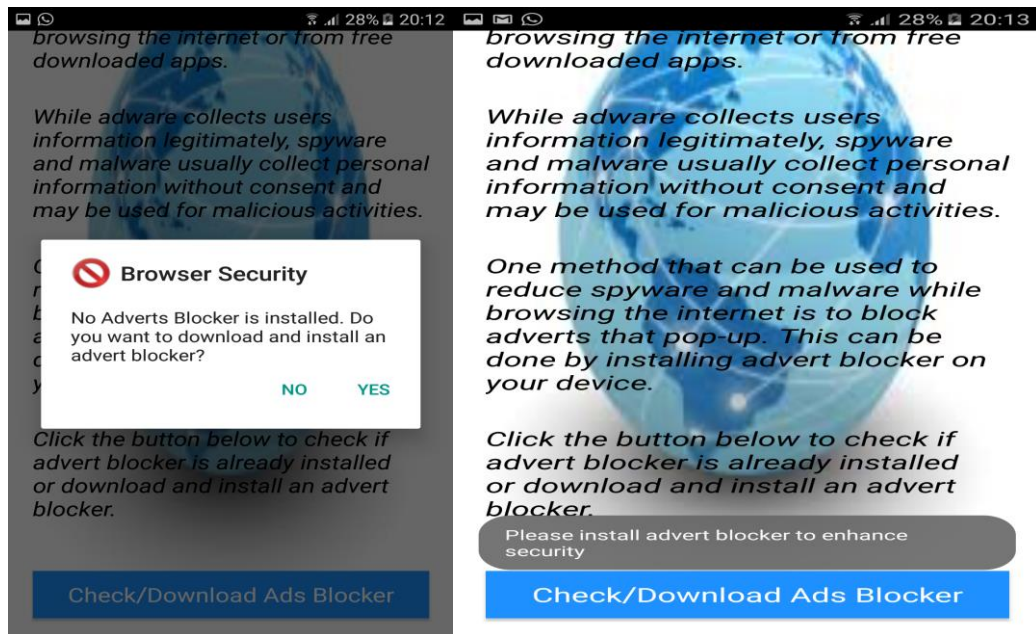


Figure 7.12: Browsing Securely

7.4.8 Regular updates

This functionality works by performing regular updates on the device to check if the latest updates have been installed for the OS. This is beneficial as most mobile device updates come with new security features which may also fix existing vulnerability in the software. While some device manufacturers and app developers notify users about new updates available, many users ignore their message or do not bother to immediately, thereby exposing their device to security threats and missing out on important new security features. By clicking on 'Check OS update Status' as shown figure 7.13 below the app checks for the latest OS update and install it with user permission.

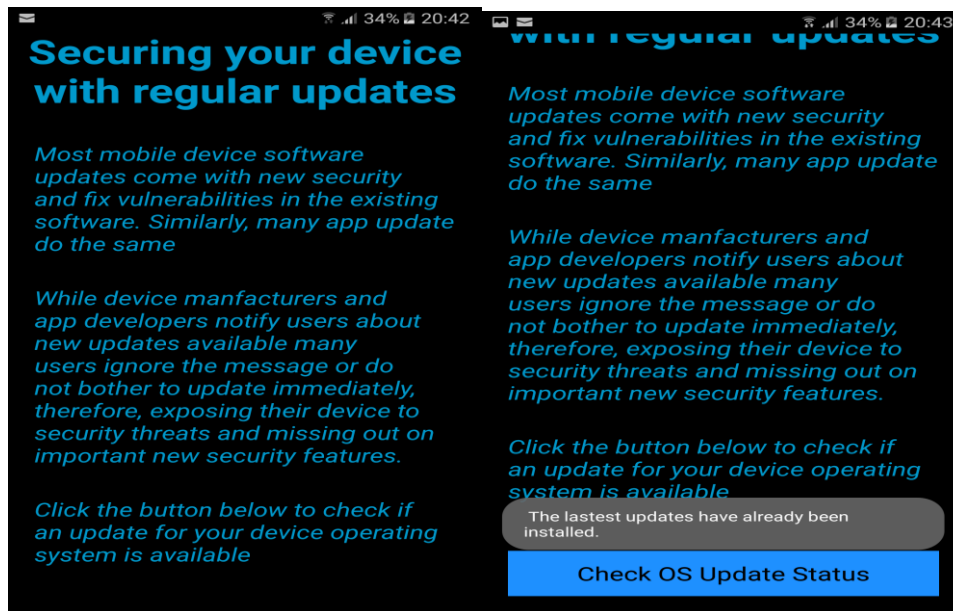


Figure 7.13: Check OS update status

7.4.9 Security Enhancement Report

The last functionality of the app is the reporting section, which provides reports on all identified security threats in the device as well as some recommendations in fixing them. The security report presents some findings on weaknesses in the m-learning device as well as making appropriate recommendations to avoid further security breaches in future (Figure 7.14). By clicking on 'Report Security Scan' from the activity list, various checks and scans results are generated from all the modules of the app that were described above and displayed on the screen. The report on functionality that are highlighted in 'Red Colour' are that the once that the users need to be concerned about and follows the recommendations on how to fix them.

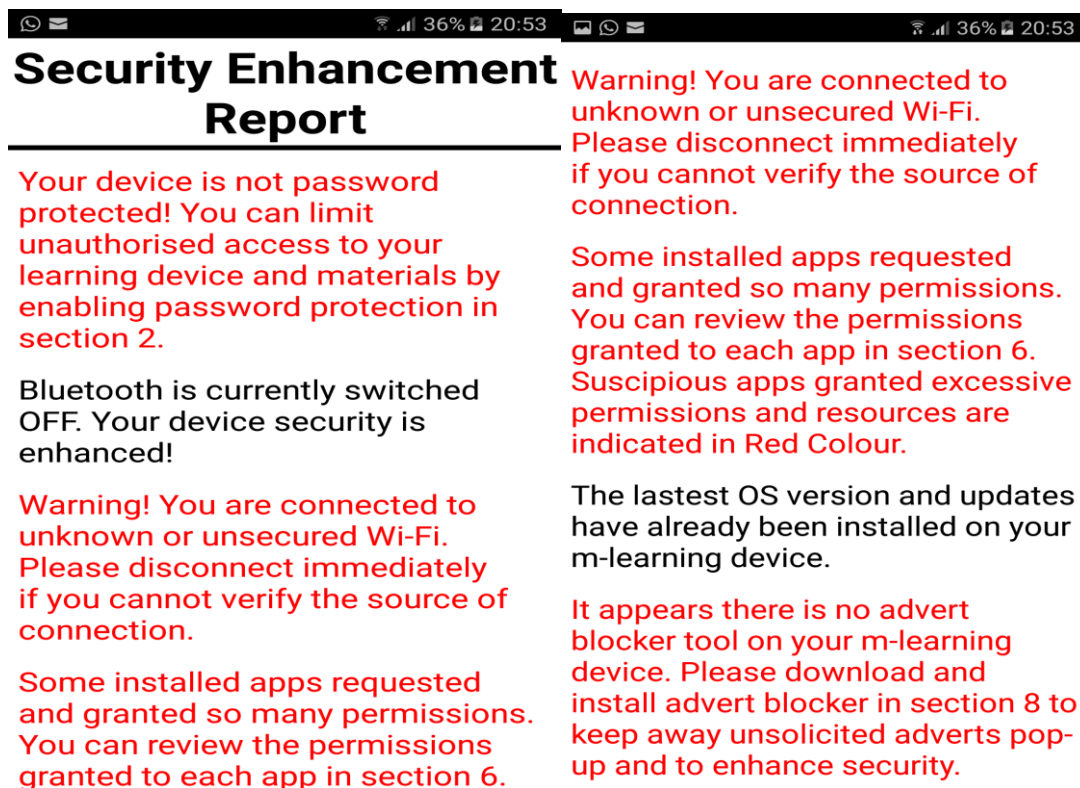


Figure 7.14: The app tips and enhancement report

7.5 The App Implementation

The first stage of the app implementation was a pilot stage where it was presented to postgraduate students for installation and use. Their initial assessment was positive, encouraging and valuable, their comments are incorporated into the actual released app for proper implementation. The main implementation stage involves distribution of the app to students and academic tutors in computer sciences in two Nigerian Universities for proper evaluation. The students who participated in the exercise were able to observe the app's features and usage. They were made aware of the security issues of their smart devices and learned some protection mechanism to reduce the risk of being exploited. Attributed to the convenience of m-learning and the daily use of their devices, students were more engaged in learning security and got insight of

the security concepts through their hands-on practices and research studies cited in the app.

7.6 The App Evaluation

7.6.1 Aims

This section aims to evaluate the usability and functionality of the security enhancement app. The evaluation was based on feedback from potential users who participated in the implementation stage.

7.6.2 Design of the evaluation method

The app was evaluated using user-centered evaluation approaches discussed in chapter three of this thesis. The evaluation took place after the app had been used for a couple of weeks in order to obtain quality feedback from the participants and to assess the app functionalities. As suggested by Oyelere *et al.* (2016), monitoring data in a mobile environment can be a challenge due to administrative, technical and conceptual limitations. Three methods are used for feedback collection and evaluation; a questionnaire/feedback form, semi-structured interviews and activity logs.

The first method is a questionnaire/feedback form which was attached to a section of the app. This is expected to be completed by all users within a period of two weeks after installation and first use. An external link to the questionnaire can be provided if requested by the participants and it consisted of three parts. Part one (See Appendix 4) was designed to understand the demographic background of the students, covering gender, age, course studied and university, all answers being optional. Part two covered mobile device security in a general form by asking questions on the user's security awareness and security app installed on their device. Part three was narrowed to the security enhancement app, starting with question on its purpose, usefulness and effectiveness. It also asked users to rate the app in terms of ease to download and use,

security awareness improvements, enhancing security of their device and contribution to security knowledge. The sections of the app were also rated on a Likert scale. All the responses gathered from the feedback form are analysed in the result section below.

The second method for data collection was a set of interviews with certain participants who are very conversant with our research work as a post-implementation study for the app and it is useful in finding out participants' opinions regarding the difficulties and problems which cannot be measured by a feedback form only. The sample group interviewed include tutors in higher education institutions in Nigeria and colleagues at the University of Warwick. The data from the interviews complement the data obtained through the feedback form. The interviews were divided into two parts. Part one was an introduction and demography collection part, explaining the purpose of the interview to the participants and signing off the consent form. It consisted of two questions obtaining demographic information from the participants. Part two consisted of the main interview questions on the security app which focused mainly on:

- The usefulness of the sections of the m-learning security enhancement app;
- Users' opinions and views on the app functionalities, awareness promotion, vulnerability scan and threats reporting;
- If the app is fit for purpose by enhancing security;
- Users' observations and suggestions on improving the app

A detailed template of the app evaluation interview question is attached in appendix 5. The third method consisted of activity logs which were set up in the app during the evaluation period to monitor the user's activities within the sections of the app. The log files help to keep track of every action the users performed within the app. Thus, it serves as a validation of the user's feedback questionnaire from the app. The log and the users' feedback are cross-checked together to validate their responses on the feedback form. The activity logs also discover a common behaviour or interest of the users in a particular section of the app through high frequency.

7.6.3 The Users' opinions – Students

A survey was carried out among 110 students, most of whom were undergraduates in Nigerian Universities as shown in Table 1 below. Most of the participants were male between 20 to 25 years old.

Table 7.1. Gender/Age group demography

| | Under 20 | 20 - 25 | 26 and over | Prefer not to say | Total |
|--------|----------|---------|-------------|-------------------|-------|
| Female | 9 | 26 | 8 | 3 | 46 |
| Male | 6 | 37 | 16 | 5 | 64 |
| Total | 15 | 63 | 24 | 8 | 110 |

An initial question was about usefulness of the app. Almost all the participants said that their security knowledge improved by tips and information given by the app on how to keep their devices safe, as shown in Figure 7.15

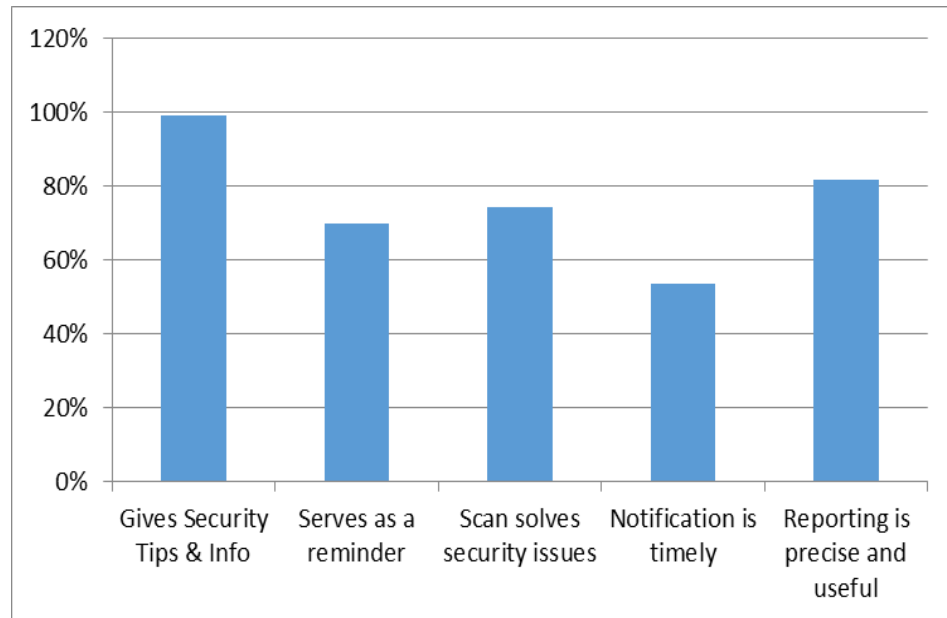


Figure 7.15: How the app is useful to the participants.

Another question was asked about the features of each section of the app. The rating of the features from the participants is shown in Figure 7.16 below. All the app functionalities except the summary section have above 70% ratings from the participants.

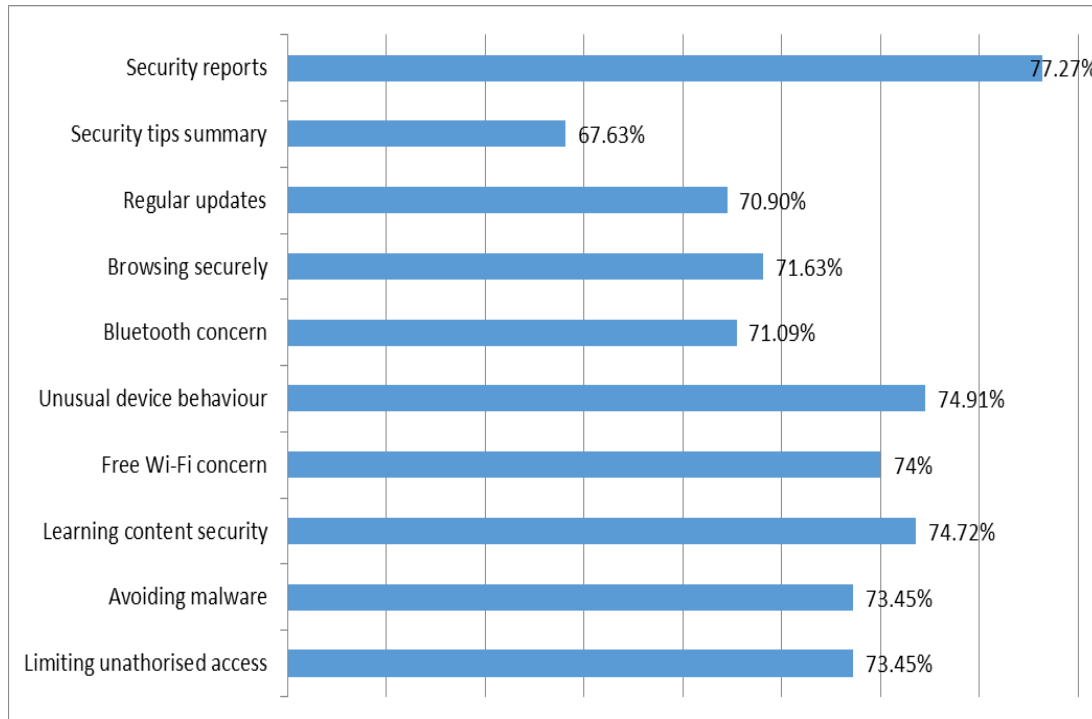


Figure 7.16: The features of the app

An interesting question from the survey also asked if the participant has experienced any security threat on their m-learning device before and if the app addressed the threat(s). 65.45% of the participants indicated that they had experienced threats before and 70.83% out of those participants said that the app addressed such security threats. An important feedback from the survey is if the security enhancement app meets the expectation of the participants and 77.27% responded 'Yes' while a meagre 2.73% responded 'No' and 20% indicated that 'They are not sure'. The last part of the questionnaire was to obtain the participants' general opinions on the functionalities

built into the app in terms of fitness for purpose, enhancement of their security, improvement in their awareness, ease to download/install and contribution to their security knowledge. The responses are shown in Figure 7.17 below.

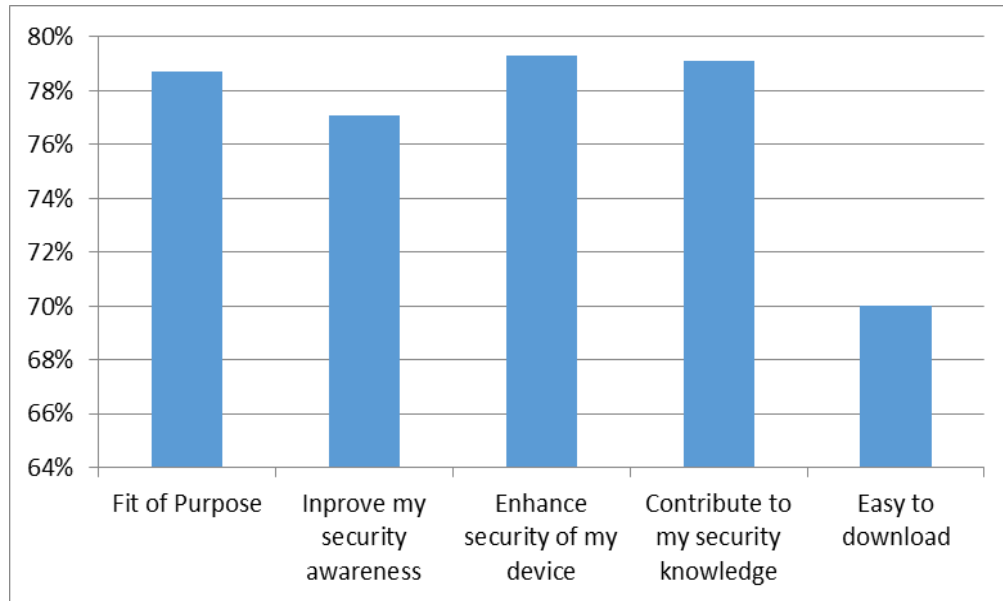


Figure 7.17: Users' opinions on the app functionalities

7.6.4 The expert opinions – Academic tutors

An evaluation interview was conducted with 15 academic staff in Nigerian Universities. Table 2 shows the demographic information about the interviewees.

Table 7.2: Gender/Age Group of interview participants

| | 30 - 39 | 40 - 49 | 50 - 59 | Total |
|--------|---------|---------|---------|-------|
| Female | 2 | 2 | 0 | 4 |
| Male | 2 | 7 | 2 | 11 |
| Total | 4 | 9 | 2 | 15 |

During the interview, four main questions were asked about the features which have been built into the app, some of which are similar to those in the questionnaire. The

first question is “which section of the app do you find very useful in terms of security?” and the response is plotted in Figure 7.18. Another question from the interview is, “which area does the app perform best in terms of awareness promotion, vulnerability scan and threat reporting?” Awareness promotion was considered the best with 66.67%, followed by vulnerability scan with 60% and lastly the report and alert with 53.33%.

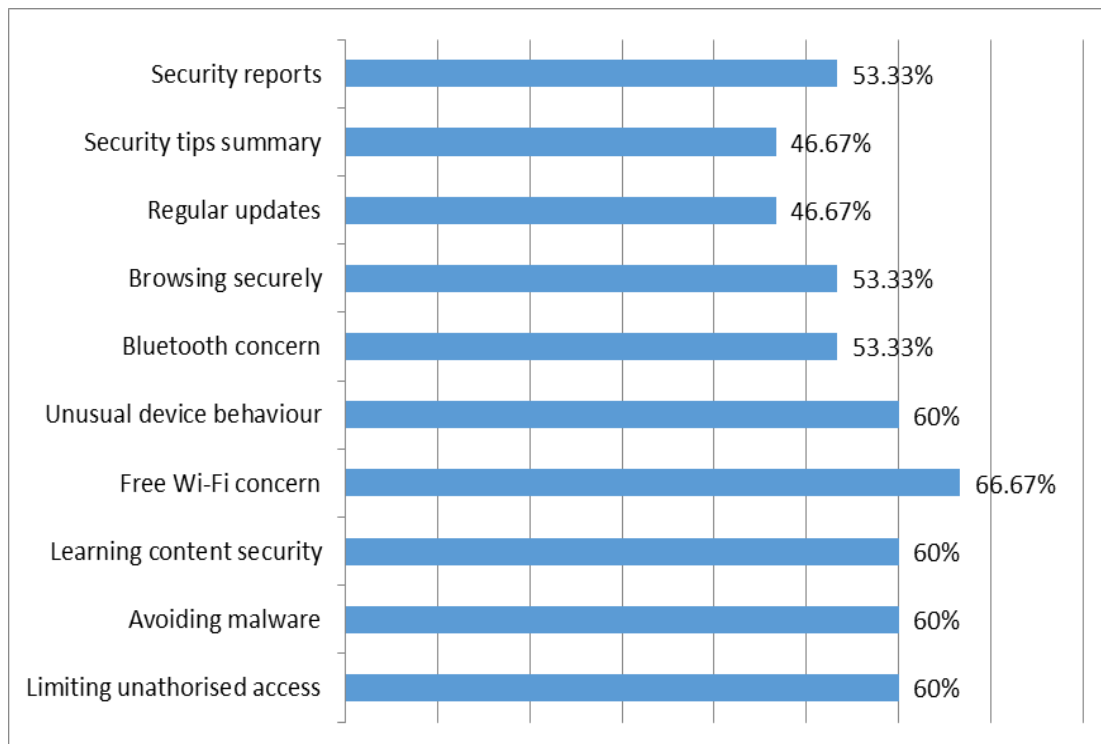


Figure 7.18: Users’ opinions on the section of the app in terms of security

Many participants also believed that all the sections of the app were purposeful because they addressed some of the prevalent security issues that are common among students in Nigerian Universities. They also found all the sections of the app very useful in term of security diagnostics and reporting. Based on various benefits of the app with reasons mentioned earlier, all the interview participants thought that the app improved the security of their devices and the learning content. They all confirmed

that the security enhancement app was fit for purpose. Further reasons given by the lecturer participants on why they think the app improves the security of their m-learning devices and why the app is fit for purpose are given in the conclusion section below.

7.6.5 Comparing Interview and Questionnaire Results

Due to similarity in some questions and feedback from questionnaires and interviews, it is necessary to compare them in order to draw a logical correlation. First to be considered are the features of the app. Figure 7.19 below shows the findings between interview (lecturers) and questionnaire (students) feedbacks.

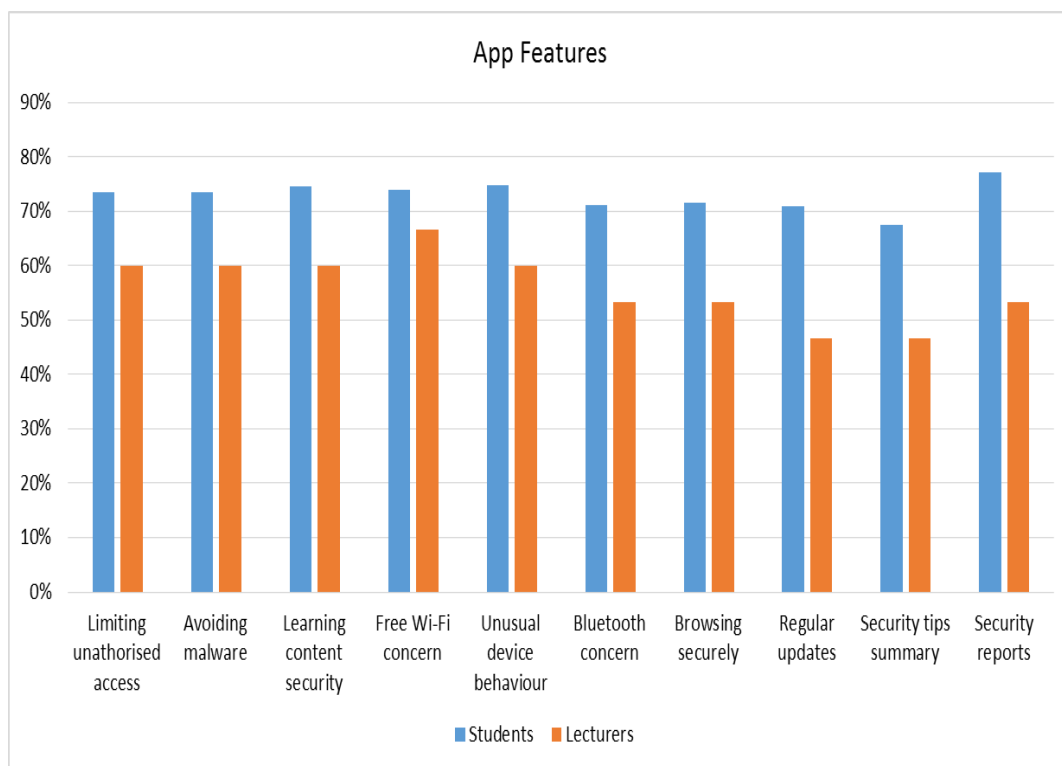


Figure 7.19: The app security features

It can be observed that the students rated all the app features higher than the lecturers. Are the students more generous and the lecturers more factual?

In comparing the app functionalities and purpose between the feedback from lecturers and students, the Figure 7.20 below says it all. While the students rated the all app functionalities higher than the lecturers, except for notifications and alerts which they rated the same, all the lecturers (100%) indicated that the security enhancement app is fit for purpose. Only 78.7% of the students shared the same view.

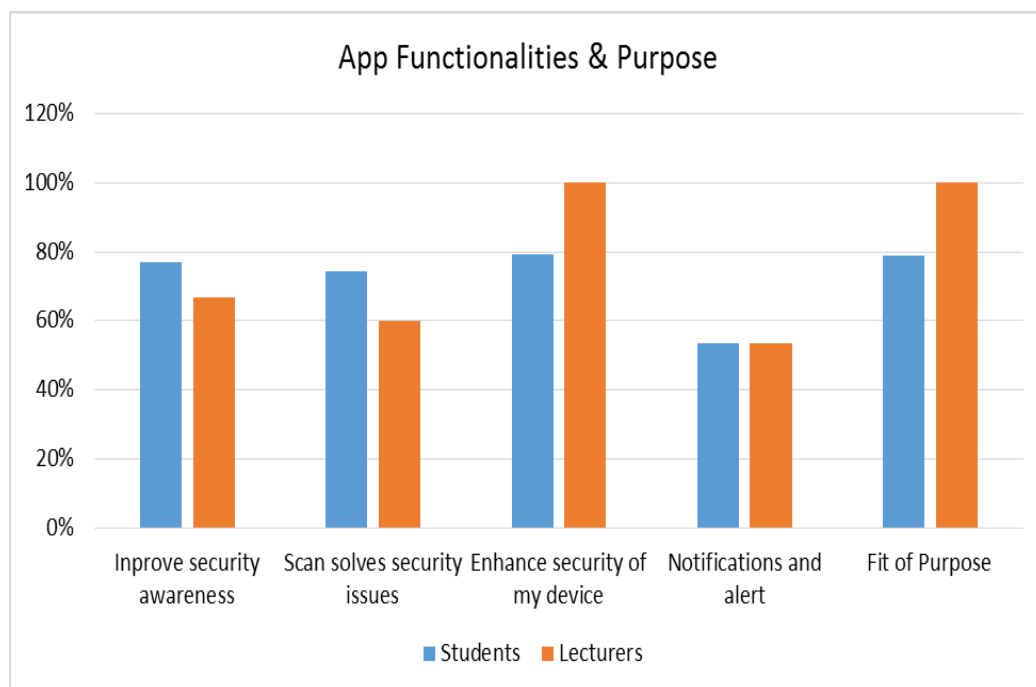


Figure 7.20: The app functionalities and purpose

7.6.6 The activity logs

The sections of the app visited by the users the during evaluation period were tracked and logged in order ascertain consistency with the feedback given by the users. While logging affected the app performance, this step is also taken to ensure reliability of

the user's responses by ensuring the sections they rated were actually explored during the implementation stage.

The results from the activity logs show that all the participants "clicked" on the "Awareness tips" sections of the app during the implementation in order to read through the security tips given and all the participants also viewed the "Security Enhancement Report" section of the app to read the summary of security checks performed on their devices. However, the scan/check activity log did not record 100% in all its sections. Very high but varying percentages were obtained on the scans/checks activity logs with the least being 94% in "Learning Content Security – Lock Documents" as shown in table 7.4 below.

Table 7.3 The app scan/check activity logs table

| Activity - Scans/Checks | Frequency | Percentage |
|------------------------------|-----------|------------|
| Limiting Unauthorised Access | 110 | 100% |
| Avoiding Malware | 110 | 100% |
| Learning Content Security | 104 | 94.50% |
| Free Wi-Fi | 110 | 100% |
| Unusual Behaviour | 106 | 96.30% |
| Bluetooth Security | 108 | 100.00% |
| Browsing Securely | 108 | 98.10% |
| Regular Updates | 106 | 96.30% |

Since the "Awareness tips" and "Security Enhancement Report" sections of the app recorded 100% activity logs and "Scan/Check" sections recorded very high percentages, which means most of the students carried out the activities expected of them during the implementation and they evaluated the app based on their experiences. Thus the results from the questionnaire/ feedback form on the security enhancement app appear to be consistent, valid and reliable when basing them on the result from the activity logs.

7.7 Discussion

Taking the security features of the app in turn, some respondents indicated that ‘Limiting unauthorised access and learning content security’ are useful to the students because of its file-lock and password mechanism which are related to some area in computer security syllabus. 60% of the participants said that they found ‘Avoiding malware and unusual behaviour’ helpful because they had issues with malware before and would do anything to avoid it. Some participants also think it is beneficial because of the scanning functionality for vulnerability of the installed apps and the notification alerts, after starting the service scanner, are good. Two-third of the participants indicated that ‘Free Wi-Fi Concern’ is the most useful part because they can connect to any available free hotspot without thinking about security. The app feature is also educative for many students who always look for free Wi-Fi to connect to regardless of security implications. Just above half of the participants found the Bluetooth security feature interesting because they often forget to disable Bluetooth after use and also browsing securely section because they have had issues with advert pop ups on our devices before. Information on how to block pop ups is a good idea to them.

Significantly, many of the participants believed that all the sections of the app are equally good and useful since they perform different activities which are necessary in providing adequate security for m-learning devices and that all the sections of the app are educative, informative and valuable. Regarding the area in which the app performs best in terms of awareness promotion, vulnerability scans and threat reporting, some of the academic participants indicated that the best module of the app is the awareness promotion because of the following reasons.

- It improves students’ education on keeping their m-learning device;
- It complements their efforts in passing knowledge to the students because it enlightens the students about their mobile device security;

- The awareness on the danger of learning the Bluetooth on and as well as the research figure to support your claim is educative;
- It reminds the students that adware and spyware spread while downloading some free apps;
- From the tutors' discussion with students who used the app, some of them (the students) expressed that they have gained security knowledge through the use of the app.

Some of the participants chose the vulnerability scan and check functionality because of the following reasons.

- Scanning app permissions is an interesting way to detect suspicious or malware infected app.
- The security scans/checks show the vulnerabilities and threats in their mobile device.
- The vulnerability scan performs best because it can detect potential security threats in apps and the device OS.
- Some are fascinated by the vulnerability scan as they use the check and scan to identify any security issue.
- The vulnerability scan is the most important part because it is where the actual security weakness identification and protection take place.
- One participant said, 'through the app, I enjoy testing the Wi-Fi connection anywhere I go by checking the Wi-Fi security'.
- Another participant said 'with the use of the app, my knowledge on adware and spyware has improved. I have also installed advert blocker as recommended, thus prevent advert pop ups on my screen unnecessarily'.

Many participants also indicated that the awareness tip and vulnerability scans are great features of the app because they serve as ‘learn and practice’ security sessions. Meanwhile many participants preferred the reporting section because the report identifies all the threats or security lapses in their device at once and provides suitable recommendations. The report also serves as a summary of all the results of the scans/checks features of the app. One participant observed that the report is interesting because the threats are highlighted in red colour, making him to pay more attention to them.

In summary, the evaluation study was successful because it gave us some feedback on what the students and educators think about our m-learning enhancement app, helped us determine whether they find the features devices useful and their opinion on the role of securing m-learning in education to reduce threats as stated in our RQ 3 in chapter one. It should, however, be pointed out that the sample size of this study limits generalization of the results; nevertheless, it does give a first glimpse on understanding the importance of m-learning security in higher education with Nigerian students.

7.8 Recommendations from the evaluation

There are many opinions which respondents made about the app, all of which are positive ones, the general opinion is that it is a good, simple, educative security app that is easy to use and understand by anyone who is interested in securing their sensitive information and learning contents, as they will find the app resourceful. Further, the app is excellent in reminding students about taking necessary precautions when using their devices and everyone who is security conscious will find the app impressive. Another opinion about the app that is worth mentioning is quoted as: **‘I really like the app functionalities and I believe it is relevant in providing security**

services. My general opinion is that the app can be relied upon as a good security tool in protecting mobile devices’.

Despite the good rating, some recommendations and suggestions on improving the app are as follows.

- Modern biometric security features may be incorporated into the app such as finger prints and voice recognition instead of convectional file lockers and password mechanisms.
- More security notification alerts should be added to other sections of the app aside the unusual behaviour section.
- The app should include prompt notification alerts to Bluetooth and Wi-Fi sections if possible, rather than scanning fully before alert.
- Security issues on copyright materials can be included in future. That is, copyrighted soft copy should not be shared without the author’s permission, as managed by DRM
- The app should distinguish real malware from other process and memory intensive app.
- The developers should keep updating the app in line with future security threats.

7.9 Summary

Mobile devices have been playing vital roles in modern day education delivery as students can access or download learning materials on their smartphones and tablets, they can also install educational apps and study anytime, anywhere. The need to provide adequate security for portable devices being used for learning cannot be underestimated.

We felt that the development of m-learning security enhancement app was necessary in order to raise students’ awareness, augment existing security in m-learning devices

and provide information on threats. The enhancement app discussed in this chapter provides security education and awareness among the students who engage their mobile devices for learning, this in turns is able to provide solution to RQ3 on reducing security threats in m-learning. By making the students aware of possible security threats, they are able to understand and recognise the threats when the threats appear, thus they are able to prevent and reduce such threats. The app helps in securing the learning contents on the portable devices through file-lock mechanisms and gives students and teachers alike the opportunity to practice simple security tasks. The security enhancement app does weakness checks or scans and offers appropriate recommendations. Through the lock mechanism and weakness checks students have been equipped with basic tools to avoid some threats, thus they have been able to prevent or reduce potential m-learning threats as stated in RQ3 in chapter one.

The monitoring facility of the app helps to monitor other apps which may be malware or spyware, through the scanner services and sends regular notifications to the users regarding any security issues or suspicious app. The ability of the students to use the monitoring facility of the app is an effort in reducing the propagation of malware or spyware in their device as well as reducing the spread the malware when exchanging files among themselves. This consequentially reduce security threats within the m-learning environment, and thus provides solution to RQ 3.

In conclusion, the app is considered fit for purpose because it helps to solve some of the security issues that students have encountered in the past or possibly likely to encounter in future. Using the app to solve past security issues is one of the ways to prevent or reduce future occurrence. We are therefore satisfied that the RQ 3 on reducing m-learning threats have been tackled by our security enhancement app and above all, the app does what it says as it provides extra security facilities in addition to normal device security. Thus, the app enhances the in-built security features of mobile devices. **Based on the evaluation results, the app also complies with the TAM principles of usability and usefulness.**

CHAPTER VIII

Other M-learning Challenges in Nigeria

8.1 *Introduction*

In the previous chapters, we have discussed security issues that affect the adoption of m-learning in HEIs in Nigeria which were identified through the various studies conducted by the researcher. We have also provided recommendations and interventions on how to reduce the security issues. In this chapter, we investigate other challenges being faced by providers or educational institutions when adopting m-learning in Nigeria. Researchers have indicated that the challenges facing the adoption of m-learning are not the same in all countries due to the levels of awareness of the technology, availability of infrastructure, the expertise in the mobile technology and the willingness of the stakeholders to implement and use the technology (Agbatogun, 2013). Although m-learning is being introduced gradually in universities across Nigeria, it is a growing form of knowledge delivery and it faces many challenges such as integration of m-learning into the existing educational curriculum and development of highly rich m-learning content.

These challenges, which are not only technologically dependent but also individually, economically and politically induced, require robust solutions in order to successfully implement secured m-learning environments in Nigerian universities. Therefore, apart from security issues that have been thoroughly examined in previous chapters, this chapter identifies and discusses other barriers and challenges being encountered when implementing m-learning, by means of a comprehensive review and survey study carried out in the HEIs. This chapter provides solution to RQ 4 in chapter one on other m-learning challenges that exist in the Nigerian education sector apart from the security threats.

8.2 Methodology

In understanding the challenges impeding m-learning adoption a user-centred methodological approach discussed in chapters three and four was employed in this study. All the participants in the initial study in chapter four were the same participants for this study, thus the students and the teachers are the focused participants, since they are the main users.

8.3 The findings

Figure 8.1 shows the results obtained from the study conducted to identify other barriers of m-learning in Nigeria. The various results obtained from the study and issues raised are discussed below.

8.3.1 Curriculum alignment

One of the challenges of adopting m-learning in Nigerian universities is the modification and alignment of the curriculum to accommodate mobile learning. Almost six out of ten of the participants (57.33%) agreed on this. While university administrators will have to modify the existing curriculum for the context of m-learning, the academics will need to integrate the new technology into their modules. The alignment of science and engineering programmes is quite complex due to laboratory practical involvement, however, art and humanity programmes can easily be aligned. The challenges of aligning m-learning in the Nigerian National Curriculum were also emphasised by Adedaja *et al.* (2012, pp.8) who stated that “some challenges are that the service would need to be aligned to the Nigerian National curriculum for all subjects offered”. Although, the curriculum redesign and alignment can be done smoothly, Kneil-Boxley (2012) remarked that many instructors often hesitate to integrate new technology into their modules until they have evidence that it will benefit their teaching experience and enhance students’

learning. The effect of their hesitation can delay implementation and adoption of m-learning or even bring it to a halt, also Cant and Bothma (2010) observed that lecturers are important in effective content delivery in the university and successful integration of technologies in education is normally influenced by their perceptions.

8.3.2 Excessive Reliance on Mobile Devices

The survey revealed that over a third of the participants (36%), mostly the educators, believed that students could rely more on mobile devices than attending classes when they were aware that they can access learning materials through their mobiles. While this practice was not a bad idea per se, the effect is that students will certainly miss out on important discussions in the classroom or any other useful activities such as impromptu quizzes being organised by their lecturers. Some educators tried to prevent the students' reliance on mobile devices being a substitute to classroom attendance by not putting learning content and materials online.

In addition, some of the academics are of the view that m-learning will only enhance the students' expertise in the use of mobile devices rather than using it to support their learning. Therefore, the effect of excessive reliance on m-learning is that student learning time and academic performance can be hampered as valuable time will be wasted learning the use of the tool instead of studying. While that is an indicated view of the academics on the matter, their opinion is supported by the findings of Osang *et al.* (2013) wherein the educators believe that technologies usually create expertise in that technology rather than the actual knowledge it is meant to deliver.

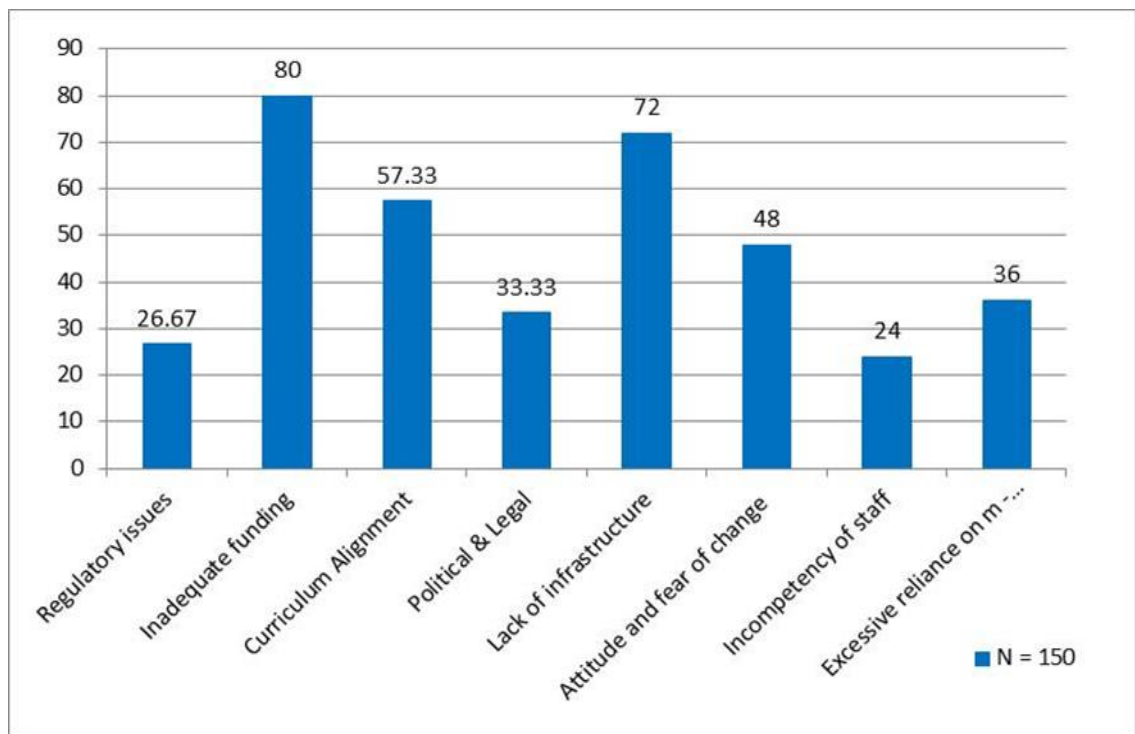


Figure 8.1: Barriers to m-learning adoption in Nigeria Universities

8.3.3 Incompetency of Staff

Another obstacle for developing content-rich m-learning in Nigerian Universities is lack of competent staff on m-learning systems as revealed by the opinion of around a quarter of the participants (24%). While mobile devices are useful in education both as administration and organisation tools, they are hardly used in delivering rich learning content. Chaka and Govender (2017) observed that m-learning is more used for information dissemination and communication, and that the strength of m-learning lies on being a method of communication rather than a content rich approach, due to lack of technical mobile developers or lack of interest in developing learning content on mobile devices. This result is also consistent with that obtained on studies conducted on e-learning and the use of digital technologies in learning in Nigeria wherein the authors concluded that lack of comprehensive and adequate knowledge of modern technologies among most Nigerian information professionals is

inimical to the success of e-learning, and the issue has been a recurring factor (Manir, 2009). The effect is m-learning is only used for information dissemination and communication instead of being a learning portal.

Perhaps, if there are no technical personnel to develop efficient and effective m-learning systems, then importation or buying off from the shelf from a developed country is a possible recommendation. However, Issa *et al.* (2011) remarked that even after learning technologies were imported into the country, lack of experts to provide technical support for the academic users could be a hindrance. The result of the study is also in line with Okeke and Umoru (2012) observed that lack of competent staff can derail mobile learning programs in Nigeria.

8.3.4 Lack of Infrastructure

More than seven out of ten of the respondents (72%) were in agreement that another major constraint to m-learning in Nigeria is lack of infrastructure to support its implementation as well as the existence of an irregular power supply, which is constantly needed to power the m-learning servers and network devices. Nigeria is a country characterised by regular power outages on a daily basis in all cities, and this has negative effects on all developmental projects including m-learning implementation. The effect is that an m-learning system cannot survive or achieve its utmost objective in this kind of an unfortunate situation. Similarly, developing and sustaining a reliable and productive m-learning system depends on the provision of proper m-learning infrastructure which includes hardware, software and good connectivity, all of which constitute a barrier to m-learning in Nigeria. This result is in line with the studies of Olugbenga (2015) and Osinaike and Adekunmisi (2012) in which the authors believe that lack of infrastructure is of one the barriers that influence the use of technology in education in Nigeria.

8.3.5 Inadequate Funding

The vast majority of the participants, eight out of ten (80%) believed that gross under-funding of the education sector, as well as its near total neglect by government, is one of the issues of main concern to stakeholders. The problem of inadequate funding has affected all aspects of education from primary to tertiary to the extent that it is usually reported in all articles on problems and challenges of education in Nigeria. Perhaps, if the classroom teaching and learning in mainstream education is so neglected, one should wonder about the fate of mobile learning in Nigeria. Anaduaka and Okafor (2013) observed that the problem of funding being faced by educational institutions has a devastating effect on the development of learning technologies including mobile learning. This study is also consistent with the findings of Osang *et al.* (2013) in which a similar proportion (75%) of the educators believe that a poor learning environment resulting from inadequate funding will affect teaching and learning activities and it is one of barriers to m-learning in Nigeria. It must be noted that the inadequate funding does not affect the private universities as much as it affects the state institutions, however, government owned tertiary institutions accounted for the highest number in the country.

4.3.6 Attitudinal Barrier

Attitude and fear of change is one of the issues raised in the survey as a barrier to effective implementation of m-learning in Nigeria. Nearly half of respondents (48%) said unwillingness to change on the side of learners and lecturers, mostly due to 'business as usual syndrome' or fear of failure is a major barrier. Many of the elderly academic staff in Nigerian Universities were trained with pen and paper for lecturing and research, and they are comfortable to continue to use them for knowledge delivery and they are not willing to change (Adegbiya and Bola, 2015). They show undue resistance to using modern learning technologies as they have not been properly trained to use them. Another reason obtained from the study for their attitude

is additional responsibility in terms of preparation for m-learning along with classroom teaching, thereby giving them extra workload without motivation. The effect is lacking behind in development in education in terms of learning technologies and innovative research. Similarly, some mature students are also not willing to embrace technology when learning as they are mainly studying for promotion at work rather than skill acquisition. This result is consistent with that obtained on a previous study on e-learning in which the author stated that lukewarm attitudes on the side of the staff and students in the e-learning processes is a challenge to successful implementation in Nigeria (Manir, 2009) as well as the result of the study obtained by Agbatogun (2013) on the use of Interactive digital technologies in Southwest Nigerian universities being impeded by lack of motivation for the faculty members. Another notable reason for the unenthusiastic attitude of lecturers is that mobile devices take learning out of the classroom beyond the reach of the lecturers, and this can be seen as a threat and loss of control. This reason is also supported by Hashemi *et al.* (2011). Meanwhile, Osang *et al.* (2013) remarked that the acceptance and readiness to use mobile technology by teaching staff and their students is a crucial factor that will determine the success rate of mobile learning implementation in Nigeria.

8.3.7 Regulatory Issues

Around a quarter of the respondents (26.67%) believed that undue regulations on ICT and learning technologies, including mobile and e-learning from regulatory authorities such as the National Universities Commission and Ministry of Education may hamper successful implementation of m-learning in Nigeria. Their belief is due to the fact that these authorities in the past have interfered in the operation of distance and open learning programmes being conducted by many universities in late 1990s to early 2000s which eventually led to the closure of distance programmes in Nigeria. Although there is no known direct regulation that hinders the adoption of m-learning in Nigeria Universities, there is a directive from the NUC that only year one and two

students should be subjected to electronic examinations and assessments, and this directive has impacted on the full implementation on m-learning, in the aspect of learning delivery and most especially on the examination and feedback processes.

This study is also consistent with the findings of Osang *et al.* (2013) on regulatory issues as only the general subjects are open to online examinations mainly at year one and two levels. Some inter-department examinations and assessments are conducted via online methods as well. Their aim is to take advantages of fast and immediate grading through computer examinations and release of results as soon as possible.

8.3.8 Political and Legal Issues

On all national issues, political and legal processes have always been involved and they have been observed as a hindrance to viable projects in Nigeria including m-learning as agreed by a third of the participant (33.33%). The participants' opinion is due to the fact that all aspects of national programmes are being politicised. Agbatogun *et al.* (2013) remarked that the level of technology integration in Nigerian higher education institutions is dependent to a large extent on government policies. While the National Policy on education by the Government specifies that Information and Communication Technology (ICT) should be integrated into all stages of education to enhance effective modern teaching and learning, Diso (2008) observed that nothing much has been achieved regarding IT policies in Nigeria when compared to international standards.

8.4 Data Analysis of the study

Further analysis was carried out on the data collected by examining the responses of the educators and students independently as shown in Figure 8.2 below. It could be observed that the educators and students shared similar views on most of the barriers; however, a wide difference is noticed on their viewpoints on excessive reliance on mobile devices.

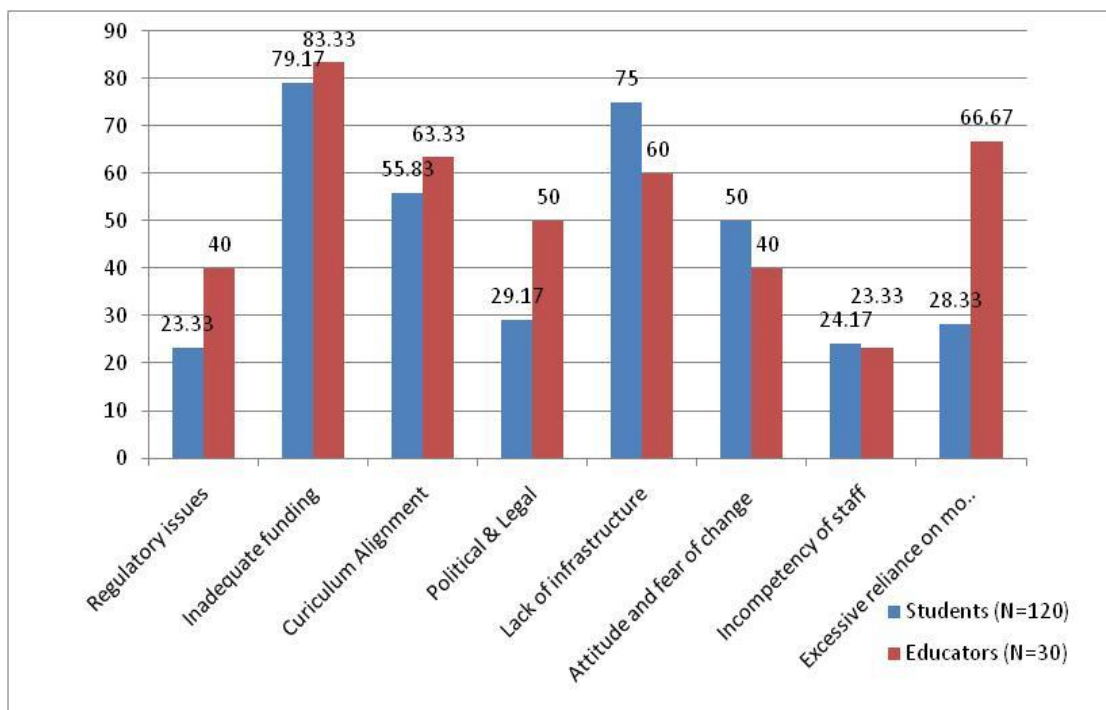


Figure. 8.2 Barriers to m-learning in Nigeria as highlighted by students and educators

This is because many of the students do not believe in excessive reliance on mobile devices or see it as a barrier to achieving their learning objectives, even though studies have stated otherwise as discussed above. Another wide discrepancy between the students and educators could be noticed on political and legal barriers. While 50% of the teachers indicated politics as a barrier, only 20.17% of the students supported this assertion. The reason for this may be that most students are not involved in Nigerian politics and they may not be aware of political hindrances to educational development in Nigeria.

8.5 Statistical and Hypothesis Testing

A statistical test was also conducted using the Mann-Whitney U Test based on the challenges on m-learning according to students and educators, who are the two main users of m-learning system. Thus the following hypothesis was tested:

H8.1: There is significant difference between the students and educators on the barriers to m-learning in HEIs in Nigeria.

Table 8.1 and 8.2 show the calculation result of the hypothesis and according to table 8.2, since the value of Z is greater than 1.96, there is significant difference between students and educators viewpoints in relation to the barriers of m-learning in Nigeria. This implies that educators and students have different views on the barriers affecting the implementation of m-learning in Nigeria and may be due to their level of education and use of mobile devices in education. In the academic environments, while the students use mobile gadgets for learning purposes, some educators make use the gadgets for teaching purposes. They both, however, use the devices for information sharing.

Table 8.1: ranking of dimension (students and educators) on the barriers of m-learning

| Dimension | Number of Participants | mean of ranks | sum of ranks | |
|-----------|------------------------|---------------|--------------|--|
| Students | 120 | 12.5 | 100 | |
| Educators | 30 | 4.5 | 36 | |
| Total | 150 | 8.5 | 136 | |

Table 8.2: Mann- Whitney test on the barriers of m-learning

| Test | The barriers of m-learning in Nigerian universities |
|--------------------|---|
| U Mann - Whitney | 0 (critical value of u is 13) |
| Z | 3.3082 |
| p-value (2-tailed) | 0.05 |

8.6 Recommendations

The above issues constitute some of the main bottlenecks for the successful implementation of m-learning in Nigeria Universities. Within this context, the following recommendations were obtained from the study as the views of the participants as possible solutions to these barriers.

- The curriculum when using a mobile learning system should be developed in collaboration with relevant stakeholders to reflect academic content and technical procedures to enhance knowledge transfer as well as provide support to learners. The curriculum outline must meet criteria to be suitable for on-line delivery, such as in engineering modules, and it must be based on content delivery and development of cognitive and social skills of the students rather than being a mere communication medium.
- The educators' interest is a crucial factor to be taken into consideration in the adoption of m-learning since they are policy drivers and stakeholders in education matters. As a way of removing attitudinal barriers, the lecturers should be trained by their employers on using modern technologies for their teaching and research job. Furthermore, the lecturers and learners should be encouraged and motivated to accept technological changes in education, either e-learning or m-learning, and inspired to have a positive attitude towards all learning technologies, m-learning inclusive. Osang *et al.* (2013) state that if educators are interested in using any technology, they will take ownership of such a project and drive it in such a way that it will be beneficial to the students and other stakeholders.
- While the use of m-learning gives students a certain amount of liberty and independence in their course of learning (El-Hussein *et al.*, 2010), it allows them to communicate with their lecturers, to interact with each other and to access course material and learning instructions while on the move or in the

comfort of their hostels. Over reliance of the students on m-learning as an alternative to classroom attendance should be avoided as much as possible. They should be made to attend classes as regularly as possible and only use m-learning to support their classroom activities. Keengwe *et al.* (2009) emphasized that teaching and learning are more effective when students are actively involved in the classroom activities. Non-attendance at lectures without genuine reasons from the student should be penalised.

- The involvement of experts and professionals in m-learning systems should be giving high consideration. Since lack of experts has been identified as a barrier, there is a need to intensify training of personnel in the field of mobile learning or engage experts from other related fields to give their valuable contribution to the development of an m-learning system. Similarly, feedback and appraisal on existing learning technologies should be taken into consideration in the development or upgrade of m-learning systems.
- The Nigerian government should as a matter of urgency address the problems of infrastructural decay in the education sector as well as the electricity supply. The future of m-learning in Nigerian Universities will look bleak if there is no adequate electricity supply to power the m-learning servers and network equipment. Adequate provision of modern infrastructures such as hardware, software, and network connectivity should also be of utmost concern.
- Since inadequate funding is listed as one of the barriers, adequate funds should be provided to Nigerian Universities to develop their m-learning facilities as well as to carry out research on how to improve the existing ones. That provision will not only boost knowledge delivery through m-learning, but also have positive impacts on Nigerian universities' global rankings.

- In tackling the regulatory issues on m-learning, the regulations on m-learning should be made in accordance with the international standards. M-learning experts in developed countries should be consulted on regulatory matters. However, the regulations should be flexible and adaptable to suit Nigerian learning environments.
- The government should give absolute priority to the education sector and m-learning in particular by creating enabling policies that will encourage growth and research in m-learning. Matters affecting m-learning, e-learning and other learning technologies should not be politicalised but be handed over to technocrats who are knowledgeable in the field.

8.7 Summary

Mobile devices have the potential to improve access to education for millions of underprivileged users in the developing world such as Nigeria, the impact of mobile learning on the life of people in developing countries appears to be more effective than people in developed countries, however, the barriers to m-learning are evidenced by deficiencies in infrastructural facilities, poor education funding, lack of motivation and unstable political problems that are common in many developing countries such as Nigeria. This chapter discusses other issues and challenges that affect the implementation and adoption of m-learning in Nigerian educational institutions apart from the security and privacy concerns which have been discussed in detail in previous publications, thus providing solutions to RQ 4 in chapter one of this thesis.

The inadequate funding from the government, most especially in the government owned educational institutions is top on the list of the barriers. It is followed by lack of infrastructure and curriculum alignment. Attitude, fear of change and incompetency of staff as well as political and legal factors also take good proportions on the list. It is obvious that the adoption of m-learning is considered to be a very

attractive option and a new learning paradigm whose effect will be a positive one to the development of education in Nigerian universities environment. If the barriers can be overcome, m-learning will enhance blended learning and improve the quality of education in the developing world, as it provides the required supplement to what is obtainable in the classroom system of learning.

CHAPTER IX

Summaries, Challenges, Contributions and Conclusion

9.1 Introduction

This study aimed at conducting research in order to produce a new dimension to secure mobile devices that are used to support the learning process **focusing on Nigerian University environments**. The specific objectives of this study were to determine the effectiveness of the proposed model to enhance security of m-learning **in Nigeria HEIs**. The research activities in this study were carried out to identify the security issues and problems faced by both students and teachers when using mobile devices in the learning process. The first stage (Chapter four) was aimed to identify the experience of the stakeholders towards security, privacy, safety of mobile security during the learning process. The primary research was conducted with students using a quantitative questionnaire, and with teachers using qualitative interviews. The second stage of the study investigated the commonly attacked component(s) of m-learning and how m-learning devices are breached (described in chapter five).

In the third stage (Chapter six), m-learning security frameworks were designed, developed and evaluated from the study activities carried out in the previous two stages in conjunction with literature reviews in chapter two. The fourth stage of this study (Chapter seven) was implementation of the intervention app which was developed in order to reduce security incidents among students and was evaluated using log file, student feedback and quantitative questionnaire following the implementation. The fifth stage of the study was post-implementation survey of the intervention and the evaluation of the m-learning security app which were carried out using two different qualitative interview set.

Finally, in the last fifth stage (Chapter eight), study on other barriers that may affect the m-learning was carried out in order to encompass all aspects of m-learning challenges in Nigerian Educational system. The research activities were carried out

quantitatively and qualitatively using questionnaire and interviews. The following sections present the summarised discussions of the main findings of this study.

9.2 Summarised Discussions from chapters

While the researcher has given detailed discussion on his findings in the contribution chapters, this section gives summarised discussion on the main research activities that were discussed in chapters four, five, six, seven and eight.

9.2.1 Discussion on user's experiences

The results from the primary research revealed that most of the students in **Nigerian HEIs** are familiar with m-learning and already engaging their mobile devices for learning purposes. They, however raised concerns on privacy protection and threats, not only within the learning environment, but also anywhere they use their devices. While some of the students take the security of the portable devices seriously, they often neglect to use the security features regularly. Security issues raised by other stakeholders such as tutors and education providers were discussed. User's experiences on m-learning security such as virus/malware attack, unauthorised access to learning content, data interception, loss or theft of device, exploitation of security breaches, Denial of service among others as well as their effects which include loss of privacy and confidential information, loss of control and psychological effects were all discussed. This research highlighted the stakeholder's responsibilities in ensuring risk free m-learning environment in chapter four.

9.2.2 Discussion of the findings on security breaches

Various ways in which the security of mobile learning devices is breached were identified in this research and they include no password lock, Blue tooth connectivity and failure to disconnect Bluetooth when not in use, threats from untrusted Wi-Fi connections and downloading materials from untrusted sources as well as through

email attachments and web browsers, all of which were discussed in Chapter five. We also figured out that the mobile device is the most vulnerable among the three components of m-learning system. While these breaches are not peculiar to HEIs in Nigeria alone, the prevalent rate at which they occur in Nigerian among students within education system makes it worrisome to the educators and education providers. With respect to the security solution and technologies, a fewer number of the respondents use password as security technologies and none of them have antivirus as a security solution. The researcher recommends that the tutors and the students must have up-to-date security technologies in order to make their devices more secure.

The results referred to above, together with the conclusions from this study seem to support previous research, which has found that human awareness and education are needed in order to protect from threats. Jansson and Von Solms, (2011, pp.74) confirm this, as they stated “Security education, training and awareness programs have proved to be the most successful regarding protecting end users against malicious attacks”.

9.2.3 Discussion of the findings on m-learning security framework

The framework was developed as a pillar and reference for developing a secured m-learning environment. While most of the security issues and solutions in the framework were not new in the security world, the researcher provides a graphical representational link between cause-effect of CIA in m-learning system to enhance its understanding and implementation especially in Nigeria HEIs. The framework was further broken down into three sub-frameworks namely clients, servers and network according to m-learning security tier systems to ease adoption. The researcher conducted a one-shot case study (as identified earlier in the Chapter six) to validate the contextual framework by the academics by measuring its usability, acceptability

and fitness for purpose as well as presented the framework in a conference for more evaluation (Shonola and Joy, 2014).

Positive responses were obtained from the evaluation and they were quite encouraging. The recommendations from both activities (evaluation surveys and conference presentation) were put into consideration and included in the final framework and sub-frameworks in chapter six of this thesis. Our evaluations revealed that mobile device is the most prone to threats than the server and network components, thus we focussed on this and proposed a security enhancement app which was presented in chapter seven of this thesis.

9.2.4 Discussion of the findings on security enhancement app

The experiment of the security enhancement app and subsequent evaluation, which has been discussed in Chapter seven, revealed that the enhancement app can deliver a suitable enhancement to the security of the mobile devices used for learning by the students. While many of the students have expressed desire to continue using the app during the evaluation, all that may be required is to motivate and encourage the students to use the app regularly.

Many students who participated in the experiment and the evaluation of the app found the activities exciting and their experience enriching, and therefore reported high levels of interest. Based on these findings, we proposed that the security enhancement app should be downloaded, installed and used by the students in securing their mobile devices along with any in-built security that comes with their gadgets. The overall findings from the student feedback confirmed that the enhanced security and privacy provided by the app may encourage the students to use it.

9.2.5 Discussion of the findings on other challenges

The results from this research show that other challenges of m-learning in HEIs may be technologically dependent, economically and politically induced as well as individual experience. The technological dependent barriers include curriculum alignment, excessive reliance on mobile devices by the students and sub-sequent students' expertise in the use of mobile devices rather than using it to support their learning and lack of technical staff in the implementation. Lack of infrastructure, inadequate funding, regulatory issues (including political and legal) constituted the economically and politically induced challenges while attitudinal barrier on the part of the students and mainly the senior tutors are the individual known barriers. Most of these challenges are supported by some other researchers in Nigeria (Osang *et al.*, 2013; Agbatogun, 2013).

However, statistical analysis shows there is significant difference between students and educators viewpoints in relation to these challenges, which may be due to their differences in their level of education and use of mobile devices in education. While the students use mobile gadgets for learning purposes, the educators use the gadgets for teaching. Many recommendations were given in chapter eight of this thesis on how to effectively eliminate these challenges in our education sectors.

9.3 Research Challenges, Scope and Limitations

9.3.1 Challenges

While several efforts were made to obtain contemporary literature on m-learning in Nigerian HEIs context, some of the articles and journals cited in this thesis are relatively old, that is more than five years. This is because the journals referenced are the ones found relevant within the context of discussion in those chapters. Furthermore, m-learning is relatively new to Nigerian education

systems, getting contemporary articles and journal publications on m-learning security suitable within Nigerian HEIs context is probably not feasible.

Getting participants for studies is sometimes a very difficult task. Many of the academic staff have busy schedule and getting hold of them for interviews is not always easy even after arranging appointments with them. On some occasions, those appointments could be changed with no notice and the researcher may have to wait for long time to be re-arrange for another interview. Cautions were normally applied when approaching the students as the Departments has to ensure that lessons are not disturbed. Sometimes extra permissions have to be taken from the teachers in order to carry out survey immediately after their classes with the students. This also meant that the researcher could not conduct studies spanning over long periods that would enable him to assess results based on long intervals particularly during the invention evaluation exercise.

Travelling to and from Nigeria to carry out the research study was another challenge. The researcher has to do the experiments in Nigeria as the sample of all the studies are Nigerian students, it was difficult for the researcher to travel for each survey activity as he is living in the UK during the PhD period. The researcher was obliged to invest her own skills, time and money, even though there were limited budget and resources available for the researcher.

9.3.2 Study Scope

The scope of this project is to carry out detailed research on different types of mobile learning security threats or risks, spot the effects of mobile security threats and the dangers caused by such threats. It furthers identify ways to prevent the threats, and carry out surveys on factors affecting the spread of mobile device security threats.

The participants of the study were limited to students currently studying in universities in Nigeria for a degree in computer science. The students are

believed to have completed a taught module in computer security and have prerequisite knowledge in mobile application devices. This is to improve the quality of the data gathered and the results obtained from the surveys as computer science students are believed to have a good understanding of the some of terminology in the questionnaires.

In addition to the students, the study subjects included tutors in computer science modules or other related modules. Lecturers who have undertaken taught modules in e-learning or distance learning are highly considered as subjects in the surveys. Other lecturers from different departments with a genuine interest in m-learning are also considered for participation.

9.3.3 Limitations

As expected in every research work and study, the followings are the limitations of this research work. It also includes problems encountered during the data collections as well as what are done to overcome them.

- 1- The security enhancement app presented as the IT solution and intervention to reduce the m-learning security threats among students was developed for Android smartphone and tablets, therefore it is limited to Android users. While this may not be a limitation per se as a study conducted as part of the initial survey showed that 92% of the students have Android devices and this is expected to grow in the future. Thus only 8% of the may not benefit of this intervention.
- 2- **During the preliminary survey, the participants were asked to answer the questions from experience they have had when using mobile devices for learning purposes only, however some participants might have answered the questions based on their perceptions or theoretical knowledge rather than security issues they have encountered before when using their mobile devices supposes.**

- 3- Location of Study: Nigeria as an independent country is divided into six geopolitical zones namely; North West, North East, North Central, South West, South East and South-South. This study could have been conducted in universities across the six geopolitical zones, but due to insecurity in five of the zones, the study was limited to South West which is known as the only safe zone. While religious conflicts, bombings and terrorism are prevalent in North West, North East and North Central zones, kidnappings are common in the South East and South South zones. In particular, the study was carried out in HEIs in Lagos state which is the most populated state, being the commercial hub as well as the former capital of Nigeria.
- 4- Practical use of mobile devices for learning: As previously mentioned in chapter 5, the study is limited to computer science students mostly in year 3 or final year, who are have been taught some modules in computer security and mobile devices. While most of the students are aware of mobile learning, some of them only have practical experience of the use computer for online examinations. Therefore, some of the responses given by the students to the questionnaire may be subjective to theoretical knowledge rather than practical involvement.
- 5- Knowledge Bias: Responses of the participants and respondents most especially during interview are limited to their knowledge of the subject matter and their mood at the time. Therefore, there is some form of subjectivity in answers given to the interview questions.

9.4 *Research contributions and significant*

9.4.1 Significance of research

Once the research is completed, a number of stakeholders will benefit from its results. First, the information gained from this findings or results of this research will provide university owners, administrators and managers with knowledge about the level of

mobile security and threats within m-learning environment. They can therefore, considers information and the research results provided as basis for developing highly secured mobile learning apps and systems.

Second, academics and researchers worldwide, particularly in Nigeria can add to their libraries another set of peer reviewed conference papers and journal publications which I have already published in relation to this research. My journals and conference papers are already being referenced in other scholar publications.

Third, our research gives further insight into how new technologies such as mobile gadgets or devices may be incorporated into educational activities to support students' learning whilst considering other barriers apart from security when implementing mobile learning in Nigerian Universities.

Fourth, this research is significant to HEIs in Nigeria, particularly to the students who are victims of security issues in m-learning. This research has investigated the manners in which the threats occur and offers solutions to the common ones. The findings of this research work will help students to overcome some of these issues.

Fifth, the reason for high security threat is lack of awareness and education on mobile device security on the part of the students. The security enhancement app is designed to raise security awareness among students. The app will also enhance security of m-learning devices by checking and scanning for vulnerabilities and rectify some issues in their devices.

9.4.2 Contribution to Knowledge

The researcher has contributed to knowledge through the development of m-learning security frameworks while complying with TAM principles and the Generally Accepted System Security Principles (GASSP) as discussed in Chapter four and which has been evaluated in order to validate the

acceptability, usability and usefulness of the frameworks I developed based on Technology Acceptance Model (TAM) principles of usefulness and usability, particularly for Nigerian HEIs. The researcher has also contributed through the development of a security enhancement app that could help to improve security awareness among students and reduces security breaches. The app could also be adapted to teaching basic security concepts to students.

The Technology Acceptance Model predicts whether users will ultimately use software applications based upon fundamental relationships among belief and attitudinal constructs that influence usage behaviour. The m-learning security enhancement app supports the two principles of TAM which are usability and usefulness. As usability is the degree of the level a system can be used by particular users to achieve specific goals in a particular context of use, majority of the users find the app useful in enhancing the security of their mobile devices as obtained in the evaluation study of the app. Furthermore, the participants in the evaluation study also indicated that enhancement app is useful and fit for purpose. Therefore, the development and evaluation of the security enhancement app as detailed in chapter seven largely comply with the Technology Acceptance Model of the principle of usability and usefulness.

9.4.3 Dissemination of knowledge gained

Throughout the course of this study, the researcher was able accumulate a great deal of knowledge and presented his research activities within and outside the University of Warwick. Moreover, the researcher had the opportunity to present seven conference papers and publish four journal articles all of which are highlighted in chapter one of this thesis.

9.4.4 Generalization of results

While this study was focused on security implication of using mobile devices for learning in Nigeria Higher education context as the research was based on data gathered from Nigerian Universities, the results obtained can be generalized to some developing countries in Africa, most especially the English speaking countries in West Africa such as Ghana and Gambia which have similar cultural backgrounds. These countries also share some of the security issues such as DoS due to power outage as irregular power outage is common in these countries.

9.5 *Conclusion and Future research*

The aim of this research was to create an enabling and a positive m-learning environment for using mobile devices teaching and learning, especially with students in Nigerian higher education institutions. The findings of this investigation, together with the intervention outcome have enabled the researcher to successfully achieve this aim. The study was able to empirically demonstrate, and validate the m-learning security frameworks which could be used as a basis to develop a new idea for successful implementation of a secured mobile learning environment.

The overall findings and outcome of this study is that security of m-learning system promotes acceptability and usability of mobile devices within learning. These results are very encouraging for the use of secure portable gadget in learning. The main results may be translated into actions to be implemented, so as to improve the adoption of smartphones and tablets within learning environments. The study has also demonstrated the security enhancement app as a suitable solution for the lack of awareness among students in the learning environment, and can help to keep students up-to-date with security issues along with the standard security settings in their mobile devices.

9.5.1 Suggestions for future research

Recommendations given to the researcher include further expansion of this study to different Universities in Nigeria and to other universities within the sub-Saharan African countries, in order to determine if similar security issues are experienced in those regions and if the solutions presented in the thesis could be adopted in different academic environments. It was also recommended for the researcher to gather more data to validate the m-learning frameworks, and in particular the intervention app. Having more data for evaluation and testing will enable the researcher to establish consistency in his results.

Bibliography

Aboderin, O.S., (2015) 'The Challenges and Prospects of E-learning in National Open University of Nigeria', *Journal of Education and Learning (EduLearn)*, Vol 9, No. 3, pp.207-216.

Adedoya, G., Botha, A., and Ogunleye, O. S. (2012), 'The future of mobile learning in the Nigerian education system', *IST-Africa 2012 Conference Proceedings, Dar es Salaam, Tanzania*, 9-11 May 2012

Adegbija, M.V. and Bola, O.O (2015) 'Perception of undergraduates on the adoption of mobile technologies for learning in selected universities in Kwara state, Nigeria', *Procedia-Social and Behavioral Sciences*, Vol, 176, pp.352-356.

Aderinoye, R.A., Ojokheta, K.O. and Olojede, A.A. (2007), 'Integrating mobile learning into nomadic education programmes in Nigeria: issues and perspectives', *International Review of Research in Open and Distance Learning*, Vol. 8, No. 2, pp. 44-52

Agbatogun, A.O (2013), 'Interactive digital technologies' use in Southwest Nigerian universities', *Education Technology Research Development* (2013) 61: pp.333–357

Alsaaty, F.M., Carter, E., Abrahams, D. and Alshameri, F., 2016. Traditional Versus Online Learning in Institutions of Higher Education: Minority Business Students' Perceptions. *Business and Management Research*, Vol 5, No. 2, p.31.

Al-Fahad, F. N. (2009) 'Students' attitudes and perceptions towards the effectiveness of mobile learning in King Saud University, Saudi Arabi', *The Turkish Online Journal of Educational Technology*, Vol. 8, No.2, pp.111–119.

Allen, I. E., and Seaman, J. (2013) 'Changing Course: Ten Years of Tracking Online Education in the United States', *Babson Survey Research Group*, pp. 4-5.

Allen, I.E., and Seaman, J (2011) *Going the Distance: Online Education in the United States*. Babson Survey Research Group pp. 4-5.

Ally, M. and Prieto-Blázquez, J (2014) What is the future of mobile learning in education? *International Journal of Educational Technology in Higher Education*, Vol 11, No. 1, pp.142-151.

- Anaduaka, U.S. and Okafor, C.F (2013) The universal basic education (UBE) programme in Nigeria: problems and prospects. *Journal of Research in National Development*, Vol 11, No. 1, pp.152-157.
- Alwi, N. M, and Ip-Shing, F (2009). ‘User’s perception in information security threats in e-Learning’, *Paper presented at the 2nd International Conference of Education, Research and Innovation*. ICERI2009 Proceedings, Madrid, Spain. pp. 2345-52
- Ambient Insight Research (2009), ‘US self-paced e-Learning market’. Monroe WA: Ambient Insight Research.
- Arkorful, V. and Abaidoo, N., (2015) The role of e-learning, advantages and disadvantages of its adoption in higher education. *International Journal of Instructional Technology and Distance Learning*, Vol. 12, No. 1, pp.29-42.
- Basaeed, E.I., Berri, J., Zemerly, M.J. and Benlamri, R (2009) ‘Web-based context-aware m-learning Architecture’, *International Journal of Interactive Mobile Technology* (iJIM). Vol.1, No.1, pp.5-10
- Beauchamp, G and Kennewell, S. (2010) ‘Interactivity in the classroom and its impact on learning’, *Computers & Education*, Vol. 54, No.3, pp.759-766
- Behera, S.K (2013) E-and M-Learning: A comparative study. *International Journal on New Trends in Education and Their Implications*, Vol 4, No.3, pp.65-78.
- Berge, Z.L. and Muilenburg, L., (2013). *Handbook of mobile learning*. Routledge.
- Boyinbode, O. K. and Akinyede, R. O. (2008) ‘Mobile learning: An application of mobile and wireless technologies in Nigerian learning system’, *International Journal of computer science and network security*, Vol. 8, No. 11, pp.386-392.
- Brody, R. G., Gonzales, K., & Oldham, D. (2013), Wi-fi hotspots: secure or ripe for fraud, *Journal of Forensic Investigative Accounting*, Vol.5, No.2, pp. 27-47.
- Brusilovsky, P. (2003). *Developing adaptive educational hypermedia systems: From design models to authoring tools*. In: T. Murray, S. Blessing and S. Ainsworth (Eds.), *Authoring Tools for Advanced Technology Learning Environment*. Dordrecht: Kluwer Academic Publishers
- Bryman, A. (2012), *Social Research Methods*. 3th edition, Oxford: Oxford University Press
- Cant, M.C and Bothma, C.H (2010) The learning-technology conundrum: Lecturers’ perspectives, *Progression*, Vol.32, No. 1, pp.55–73.

Carliner, S. and Shank, P. eds (2016) *The e-learning handbook: past promises, present challenges*. John Wiley & Sons.

Carroll, J.M., (2014) *Computer security*. Butterworth-Heinemann.

Chaka, J.G. and Govender, I (2017) 'Students' perceptions and readiness towards mobile learning in colleges of education: a Nigerian perspective' *South African Journal of Education*, Vol. 37, No. 1, pp.1-12.

Cheng, W.Y.T. and Chen, C.C (2015). The Impact of e-Learning on Workplace On-the-job Training. *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 5, No.4, p.212.

Chidiogo, E (2013) 'Nigeria ranked sixth in Internet security threat' [Online] Available from <http://telegraphng.com/2013/06/nigeria-ranked-sixth-in-internet-security-threat/> [Accessed on 10-January-2014]

Childs, S., Blenkinsopp, E., Hall, A and Walton, G. (2005) 'Effective e-learning for health professionals and students – barriers and their solutions', A systematic review of the literature – findings from the HeXL project. *Health Information and Libraries Journal*, Vol. 22, No. 2, pp. 20–32

Cho, V., Cheng, T. C. E., and Lai, J. (2009), 'The role of perceived user-interface design in continued usage intention of self-paced e-Learning tools', *Computers & Education*, Vol. 53, No. 2, pp. 216–227.

Churchill, D., Lu, J., Chiu, T.K. and Fox, B (2016). *Mobile Learning Design*. Springer Singapore: Imprint: Springer,.

Clark, R.C. and Mayer, R.E., (2016) *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*. John Wiley & Sons.

Clarke, N. L., and Furnell, S. M. (2005) 'Authentication of users on mobile telephones–A survey of attitudes and practices', *Computers & Security*, Vol. 24, No. 7, pp 519-527

Cohen, L., Manion, L. and Morrison, K. (2013), *Research methods in education*. Routledge.

Creative Research System Sample size calculator [Online] Available at <http://www.surveysystem.com/sscalc.htm> [Accessed on 20 June 2016]

Creswell, J.W. and Clark, V.L.P. eds., (2011) *Designing and Conducting Mixed Methods Research*. SAGE.

Curran, C. (2004). Strategies for e-learning in universities. Available on Google Scholar.

Dag, F and Gecer, A (2009) 'Relations between online learning and learning styles', *World Conference on Educational Sciences*. Procedia Social and Behavioral Sciences 1 (2009), pp. 862–871.

Djigic, G and Stojiljkovic, S (2011). 'Classroom management styles, classroom climate and school achievement', *International Conference on Education and Education Psychology*, Istanbul, Turkey, pp. 819 – 828

Dimkov, T., Pieters, W and Hartel, P (2011) 'Portunes: representing attack scenarios spanning through the physical, digital and social domain'. In *Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security* Springer Berlin Heidelberg, 2011, pp.112-129, 2011.

Diso, L.I (2008), 'Mobile service providers and m-learning in Nigeria: mobility in a contracting Space' *International Journal of Interactive Mobile Technologies (iJIM)*, Vol.2, No. 1, pp. 40-45

Gee, D and Farb, D (2005) Link to Learn. Managed Healthcare Executive. Available at <http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/link-learn?id=&pageID=1&sk=&date=> [Accessed on 20 May 2013].

Edwards, W.K., Bellotti, V., Dey, A.K. and Newman, M.W (2003) 'The challenges of user-centered design and evaluation for infrastructure', *In Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 297-304). ACM.

El-Gamil, K and Badawy, O.M (2010) 'M-learning framework for university students', *International Conference on Computer Theory and Applications*, 23-25 October 2010, Alexandria, Egypt

El-Hussein, M. O. M., and Cronje, J. C. (2010). 'Defining Mobile Learning in the Higher Education Landscape', *Educational Technology & Society*, Vol. 13, No. 3, pp.12–21.

El-Sofany, H.F and El-Seoud, S.A. (2009). 'Towards the development of an m-learning system: A New Stage to Enhance Higher Education', *International Journal of Interactive Mobile Technology (iJIM)*, Vol.3, No. 3, pp. 4-9

Enck, W., Ongtang, M., & McDaniel, P. (2009) 'Understanding android security', *IEEE security & privacy*, No.1, pp 50-57

Evans, C. (2008) 'The effectiveness of m-learning in the form of podcast revision lectures in higher education', *Computers & Education*, Vol. 50 (2008), pp. 491–498

Fayolle, J., Gravier, C., Ates, M and Lardon, J (2009). 'Remote laboratories framework: Focus on Reusability and Security in M-learning Situations', *International Journal of Online Engineering iJOE*, Vol.5, No. 3, pp. 19-24.

Ferriman, J. (2013). The History of Distance Learning (Infographic). Learn Dash, Available online www.learndash.com/the-history-of-distance-learning. Accessed on [30 July, 2014]

Flower, A., McDaniel, S.C. and Jolivette, K., (2011). A literature review of research quality and effective practices in alternative education settings. *Education and Treatment of Children*, Vol. 34, No.4, pp.489-510

Figueredo, O.R.B. and Villamizar, J.A.J (2015). Framework for Design of Mobile Learning Strategies. In *Handbook of Mobile Teaching and Learning* (pp. 75-89). Springer Berlin Heidelberg.

Ghorbanzadeh, P., Shaddeli, A., Malekzadeh, R and Jannbakhsh, Z (2010) 'A survey of mobile database security threats and solution for IT', *3rd International Conference on Information Sciences and Interaction Sciences (ICIS)*, 23-25 June 2010, Chengdu, China. pp. 676 – 682

Greenhow, C., Robelia, B. and Hughes, J. E. (2009) 'Learning, teaching, and scholarship in a digital age Web2.0 and classroom research: what path should we take now?' *Educational Researcher*, Vol. 38, No. 4, pp. 246–259.

Giacomin, J (2014) What is human centred design?. *The Design Journal*, Vol. 1, No.4, pp.606-623.

Gikas, J. and Grant, M.M. (2013) 'Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media' *The Internet and Higher Education*, Vol. 19, pp.18-26.

Goffe, W. L., and Sosin, K. (2005). 'Teaching with technology: may you live in interesting times', *Journal of Economic Education*, Vol. 36, No. 3, pp. 278–291.

Gulati, S. (2008), 'Technology-enhanced learning in developing nations', *International Review of Research in Open and Distance Learning*. Vol. 9, No.1, pp.1–16

Gregory, P (2009), *CISSP Guide to Security Essentials*, Cengage Learning Inc. Boston.

Grönlund, A, and Islam, Y, M. (2010), 'A mobile e-learning environment for developing countries: the Bangladesh virtual interactive classroom', *Information Technology for Development*, Vol. 16, No.4, pp.244–259

GSMA (2012). Safeguarding, Security and Privacy in Mobile Education. GSMA Connected Living programme: mEducation.

Hannay, M., and Newvine, T. (2006) 'Perceptions of distance learning: A comparison of online and traditional learning', *Journal of Online Learning and Teaching*, Vol. 2, No. 1, pp. 1-11.

Hashemi, M., Azizinezhad, M., Najafi, V and Nesari A, J (2011), 'What is Mobile Learning? Challenges and Capabilities', *Procedia Social and Science Behaviour*. Vol. 30 (2011) pp. 2477 – 2481

Hasan. S. H., Alghazzawi, D. M and Zafar, A (2014) 'E-learning systems and their security' *BRIS Journal of Adv. S & T* (ISSN. 0971-9563) Vol.2, No 3, pp. 83-92

Hein, J O. (2014) A Comparison of a Blended Learning Environment and a Traditional Learning Environment. *Are Student Achievement and Student Interest Affected?*. Wilmington University (Delaware).

Howell, M., Love, S. and Turner, M. (2008) 'User characteristics and performance with automated mobile phone systems', *International Journal of Mobile Communications*, Vol. 6, No. 1, pp. 1-15.

Hussein, R., Aditiawarman, U and Mohamed, N. (2007) 'E-learning acceptance in a developing country: a case of the Indonesian Open University', *In Paper presented at the German e-Science conference*, Available at <http://edoc.mpg.de/316634>. [Accessed 18-May-2013]

Hydara, I., Sultan, A.B.M., Zulzalil, H. and Admodisastro, N (2015) Current state of research on cross-site scripting (XSS)—A systematic literature review. *Information and Software Technology*, Vol.58, pp.170-186.

IDC (2015) 'International data corporation smartphone OS market share, 2015', Q2Worldwide Quarterly Mobile Phone Tracker. Available online at <http://www.idc.com/prodserv/smartphone-os-market-share.jsp> Accessed on [24-04-2016]

Ibrahim, I., Yusoff, W, Z and Sultan Sidi, N.S., (2011). 'Space charging model: Cost analysis on classrooms in higher education institutions', *Procedia Social and Science Behaviour*. No. 28, pp. 246-25

Issa, A.O., Ayodele, A.E., Abubakar, U and Aliyu, M.B (2011) 'Application of information technology to library services at the federal university of technology, Akure library, Ondo State, Nigeria', *Library Philosophy and Practice*. <http://unllib.unl.edu/LPP/issa-ayodele-abubakarbola.pdf>. Accessed 6 October 2012.

Israel, G.D (1992) 'Determining sample size. University of Florida Cooperative Extension Service', Institute of Food and Agriculture Sciences, EDIS.

Jacob, S. and Radhai, S., (2016) 'Trends in ICT E-learning: Challenges and Expectations', *International Journal of Innovative Research and Development* Vol. 5 No.2

Jansson, K. and Von Solms, R. (2011) 'Simulating malicious emails to educate end users on-demand' in *Web Society (SWS), 2011 3rd Symposium*. Port Elizabeth, 26-28 Oct. 2011. IEEE, pp. 74-80.

Juniper (2011) 'Mobile Device Security —Emerging threats, Essential strategies', Key capabilities for safeguarding mobile devices and corporate assets. A white paper by Juniper Networks Inc.

Jang-Jaccard, J and Nepal, S (2014), 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences*, Vol. 80, pp. 973–993

Jegede, P. O. (2009) 'Age and ICT-related behaviours of higher education teachers in Nigeria', *Issues in Informing Science and Information Technology*, 6(2009), pp.770–777.

Jingde, C., Goto, Y. and Koide, M. (2007) 'Enquete-Baise: a general-purpose questionnaire server for ubiquitous questionnaire' In: *The 2nd IEEE Asia-Pacific Service Computing Conference*. Tsukuba Science City, Japan, pp.187-195.

Jokela, T., Iivari, N., Matero, J. and Karukka, M. (2003) 'The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11', In *Proceedings of the Latin American conference on Human-computer interaction* (pp. 53-60). ACM.

Kabay, M.E (2007) Security for telecommuters. [Online] Available at <http://www.securitytechnet.com/resource/rsc-center/vendor-wp/trusecure/telecommuters.pdf> 2007. [Accessed on 02-August-2012]

Kambourakis, G (2013), 'Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art' *International Journal of u- and e- Service, Science and Technology*, Vol. 6, No.3, pp.67-84

Kaplan, A. M and Haenlein, M. (2010), 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons*, Vol. 53, No.1, pp. 59-68.

Kagan, J (2014). The New wireless wave: Prices falling, cloud rising. [Online] Available from <http://www.ecommercetimes.com/story/79925.html#sthash.sMadKBnE.dpuf> [Accessed on 10-March-2014]

Keegan, D. (2005), 'The incorporation of mobile learning into mainstream education and training', *World Conference on Mobile Learning, Cape Town*.

Keegan, D. (2004). 'Mobile learning: the next generation of learning', *The 18th Asian Association of Open Universities Annual Conference, Shanghai*.

Keengwe, J, Pearson, D and Smart, K (2009). Technology integration: Mobile devices (iPods) constructivist pedagogy and student learning. *AACE Journal*, 17(4), pp.333–346. Chesapeake, VA: AACE. <http://www.editlib.org/p/29411>. [Accessed on 3 March 2014].

Kearney, M., Schuck, S., Burden, K. and Aubusson, P (2012). 'Viewing mobile learning from a pedagogical perspective', *Research in Learning Technology*. Vol.20, No.1, pp. 1-17

Keser, H., Uzunboylu, H. and Ozdamli F. (2011), 'The trends in technology supported collaborative learning studies in 21st century', *World Journal on Educational Technology*, Vol. 3, No.2, pp.103-119.

Kim, J., Lee, A. and Ryu, H., (2013) 'Personality and its effects on learning performance: Design guidelines for an adaptive e-learning system based on a user model', *International Journal of Industrial Ergonomics*, Vol. 43, No. 5, pp.450-461.

Kneil-Boxley, S (2012), 'Towards a mobile learning strategy to support Higher Education' *Innovative Practice in Higher Education*, Vol. 1, No. 2. 2012

Konstantinou, P.(2013) Rapid Application Development. Accessed on [31 July, 2016]

Kose, U (2010) 'A blended learning model supported with Web 2.0 technologies', *Procedia Social and Behavioral Sciences* No.2 (2010), pp. 2794–2802

Kraftl, P (2013) *Geographies of alternative education*. Policy Press.

Kukulska-Hulme, A., Sharples, M., Milrad, M., Arnedillo-Sánchez, I. and Vavoula, G.(2009), 'Innovation in mobile learning: A European Perspective', *International Journal of Mobile and Blended Learning*, Vol. 1, No. 1, pp. 13-35.

Kurilovas, E. and JUŠKEVIČIENĖ, A (2014) 'On recommending Web 2.0 tools to personalise learning', *Informatics in Education-An International Journal*, Vol 13, No1, pp.17-32.

Kurkovsky, S., & Syta, E. (2010), 'Digital natives and mobile phones: A survey of practices and attitudes about privacy and security', *In Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*, pp. 441-449

Larman, C. and Basili, V. R. (2003) 'Iterative and incremental development: A brief history' *IEEE Computer*, Vol.36, No.6, pp.47-56.

Lane, L (2014) Social media can aid spread of false information. [Online] Available from http://www.dailytoreador.com/opinion/article_c6496c06-87d4-11e3-b0c3-001a4bcf6878.html / [Accessed on 10-April-2014]

La Polla, M., Martinelli, F., and Sgandurra, D. (2013), 'A survey on security for mobile devices', *Communications Surveys & Tutorials IEEE*, Vol. 15, No.1, pp 446-471.

Leavitt, N. (2013) Today's Mobile Security Requires a New Approach. *IEEE Computer*, Vol. 46, No 11, pp.16-19.

Le Thanh, H. (2013), 'Analysis of malware families on Android mobiles: Detection characteristics recognizable by ordinary phone users and how to fix it', *Journal of Information Security*, Vol. 4, No.4, pp 213.

Lesser, V.M., Yang, D.K., Newton, L.D. and Sifneos, J.C (2016) 'Mixed-Mode Surveys Compared with Single Mode Surveys: Trends in Responses and Methods to Improve Completion' *Journal of Rural Social Sciences*, Vol.31, No.3, p.7.

Levy.Y., Ramim, M , M and Hackney, A.R (2013), 'Assessing ethical severity of e-learning systems security attacks', *Journal of Computer Information Systems*, Vol. 53, No.3, pp.75-84

Lim, C. C., and Jin, J. S. (2006), 'A study on applying software security to information systems: e-learning portals. *IJCSNS*, Vol. 6, No. 3B, pp.162.

Luminita, C.D.C. and Magdalena, C.I.N (2012). 'E-learning security vulnerabilities', *4th World Conference On Educational Sciences (WCES-2012)* Barcelona, Spain. pp. 2297–2301

Mao, J.Y., Vredenburg, K., Smith, P. W. and Carey, T. (2005), 'The state of user-centered design practice', *Communications of the ACM*, Vol. 48, No.3, pp.105-109.

Marforio C., Francillon A. and Capkun S (2013) Application Collusion Attack on the Permission-Based Security Model and its Implications for Modern Smartphone Systems, available online <ftp://ftp.inf.ethz.ch/doc/tech-reports/7xx/724.pdf> Accessed on [30 July, 2016]

Marangunić, N. and Granić, A. (2015) Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, Vol.14, No.1, pp.81-95.

McCarty, C., Bennett, D., and Carter, S. (2013). 'Teaching college microeconomics: Online vs. traditional classroom instruction. *Journal of Instructional Pedagogies*', Vol.11, No.1, pp. 20-28

Meehinkong, T., Praneetpolgrang, P. and Mekhabunchakij, K (2009) 'The analysis and evaluation of security readiness in ICT Infrastructure for Supporting e-Learning in Institute of Physical Education', *The Sixth International Conference on eLearning for Knowledge-Based Society* 16-17 December 2009, Bangkok, Thailand.

Mehdipour, Y. and Zerehkafi, H (2013) 'Mobile learning for education: Benefits and challenges', *International Journal of Computational Engineering Research*, Vol 3, No.6, pp.93-101.

Manuti, A., Pastore, S., Scardigno, A.F., Giancaspro, M.L. and Morciano, D., (2015). Formal and informal learning in the workplace: a research review. *International Journal of Training and Development*, Vol.19, No 1, pp.1-17.

Merkow, M.S. and Breithaupt, J (2014). *Information security: Principles and practices*. Pearson Education.

Miller, G. (2014). History of Distance Learning. Retrieved May 5, 2016 at: <http://www.worldwidelearn.com/education-articles/history-of-distance-learning.html>

Mohammadi, H., (2015) 'Investigating users' perspectives on e-learning: An integration of TAM and IS success model', *Computers in Human Behavior*, Vol. 45, pp.359-374.

Mohini, T., Kumar, S.A. and Nitesh, G. (2013) 'Review on Android and smartphone security', *Research Journal of Computer and Information Technology Sciences*, p.6527.

Mulliner, C.R (2006) Security of smartphones, Master's thesis submitted to University of California, Santa Barbara, June 2006.

National Universities Commission (NUC) (2012), 'List of Nigerian Universities and years founded' Available on <http://www.nuc.edu.ng/pages/universities.asp>. [Accessed on 30-July-2012]

Nawaz, A., (2013) 'Using e-learning as a tool for education for all in developing states', *International Journal of Science and Technology Education Research*, Vol. 4, No. 3, pp.38-46.

Negash, S, Whitman, M, E., Woszczynski, A, B., Hoganson, K and Mattord, H (2008), *Handbook of Distance Learning For Real Time And Asynchronous Information Technology Education*. Hersey, IGI Global: Information Science Reference.

Nerur, S., Mahapatra, R. and Mangalaraj, G. (2005) 'Challenges of Migrating to Agile Methodologies' *Communications of the ACM* Vol. 48, No. 5, pp.73-78.

Nordin, N., Embi, M.A. and Yunus, M.M. (2010). 'Mobile learning framework for lifelong learning. international conference on learner diversity 2010' *Procedia - Social and Behavioral Sciences*. Vol. 7, No.10, pp. 130-138.

Norman, D. A. and Draper, S. W. (1986), 'User centered system design', Erlbaum, Hillsdale, NJ

Obodoeze, F.C., Okoye, F.A., Mba, C.N., Asogwa, S.C. and Ozioko., F.E (2013) 'A Holistic Mobile Security Framework for Nigeria', *International Journal of Innovative Technology an Exploring Engineering (IJITEE)*, Vol. 2, No. 3, pp.1-11

Olugbenga, O., (2015) 'Mobile Phone As a Cost-Effective Option for M-Learning in Tertiary Education in Nigeria: Prospects and Problems', In *Society for Information Technology & Teacher Education International Conference* Vol. 2015, No. 1, pp. 1695-1700.

Okeke, A,U and Umoru, T, A. (2012) 'M-learning in Nigerian Universities: Challenges and Possibilities' *Global Awareness Society International 21st Annual Conference*, New York City

Ormrod, J.E. and Leedy, P.D (2005) *Practical research: Planning and design*, New Jersey, Pearson Merill Prentice hall.

Ooi, K.B. and Tan, G.W.H. (2016). 'Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card', *Expert Systems with Applications*, 59, pp.33-46.

Osang,B.F., Ngole, J. and Tsuma, C .(2013) 'Prospects and challenges of mobile learning implementation in Nigeria: Case Study National Open University of Nigeria (noun)', *A paper presented at International Conference on ICT for Africa 2013*, February 20 -23, Harare, Zimbabwe

Osinaike, A.B and Adekunmisi, S.R (2012) 'Use of multimedia for teaching in Nigerian university system: A case study of university of Ibadan'. Library Philosophy and Practice (e-journal).
[http://www. webpages.uidaho.edu/~mbolin/oshinaike-adekunmisi.htm](http://www.webpages.uidaho.edu/~mbolin/oshinaike-adekunmisi.htm). Accessed 6 October 2012.

Oyelere, S.S Suhonen, J and Sutinen, E (2016) 'M-Learning: A new paradigm of learning ICT in Nigeria', *International Journal of Interactive Mobile Technologies (iJIM)*, Vol. 10, No. 1, 2016

Oyelere, S.S. & Oyelere, L. S (2015) 'Users' Perception of the effects of viruses on computer systems – An Empirical Research', *African Journal of Computing and ICT*, Vol. 8, No. 1, pp.121–130

Oyelere, S.S. Paliktzoglou, V and Suhonen, J (2016) 'M-learning in Nigerian higher education: an experimental study with Edmodo', *International Journal of Social Media and Interactive Learning Environments*, Vol. 4, No. 1, pp.43–62.

Ozdamli, F (2011) 'Pedagogical framework of m-learning' *Procedia - Social and Behavioral Sciences* Vol. 31 (2012), pp. 927 – 931.

Ozkan, S., and Koseler, R. (2009). 'Multi-dimensional students' evaluation of e-learning systems in the higher education context: an empirical investigation', *Computers & Education*, Vol. 53, No.4, pp.1285–129

Ozuorcun N,C and Tabak, F. (2012) 'Is m-learning versus e-learning or are they supporting each other', *4th World Conference On Educational Sciences*, Barcelona, Spain. pp. 299-305

Page, T. (2011), 'Interaction and usability considerations in the design of mobile phones', *Journal of Design Research*, Vol.9, No.3, pp.281-300.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K., (2015) 'Purposeful sampling for qualitative data collection and analysis in mixed

method implementation research', *Administration and Policy in Mental Health and Mental Health Services Research*, Vol. 42, no.5, pp.533-544.

Paolucci, R., (2014) *Mobile Learning Environments: Readings in Open Research* CreateSpace Independent Publishing Platform.

Parsons, D., Ruy, H. and Cranshaw, M (2007) 'A design requirements framework for mobile learning environments', *A Journal of Computers*, Vol. 2, No. 4, pp. 1-8.

Pegrum, M (2014) *Mobile learning: Languages, literacies and cultures*. Springer.

Peltier, T.R., (2013) *Information security fundamentals*. CRC Press.

Picciano, A.G., Dziuban, C.D. and Graham, C.R., (2013) *Blended learning: Research perspectives* (Vol. 2). Routledge

Pieprzyk, J., Hardjono, T. and Seberry, J (2013), *Fundamentals of computer security*. Springer Science & Business Media.

Polla M.L., Martinelli F., and Sgandurra D (2013) A Survey on Security for Mobile Devices, *Communications Surveys & Tutorials*, IEEE, Vol.15, No.1, pp. 446–471

Preece, J., Sharp, H. and Rogers, Y. (2015) *Interaction Design-beyond human-computer interaction*, John Wiley, Chichester, UK

Qian, K., Lo, C. T. D., Guo, M., Bhattacharya, P., and Yang, L. (2012) 'Mobile security labware with smart devices for cybersecurity education', *In Integrated STEM Education Conference (ISEC)*, No2. pp. 1-3

Quinn, C (2000). M-Learning. Mobile, Wireless, In-Your-Pocket Learning. Available at <http://www.linezine.com/2.1/features/cqmmwiyp.htm> [Accessed on 30-July-2012]

Quintana, C., Krajcik, J., Soloway, E., Fishman, L.C.D.I.B. and O'Connor-Divelbiss, S (2013). Exploring a structured definition for learner-centered design. In *Fourth international conference of the learning sciences*, pp. 256-263

Rafiu, M. I., Kayode. S . A, and Rapheal, T. O (2011) 'Implementing mobile e-learning in Nigeria tertiary educational system – A Feasibility Study', *International Journal of Science and Advanced Technology*, Vol.1 No.1,pp. 7

Ramjan, S (2010), 'The conceptual framework of mLearning security for university in Thailand', *The Seventh International Conference on eLearning for Knowledge-Based Society*, 16-17 December 2010, Bangkok, Thailand

Ramakrisnan, P., Yahaya, Y., Hasrol, M, N. and Abdul Aziz, A (2011) ‘Blended Learning: A suitable framework for e-Learning in higher education’ *The 3rd International Conference On e-Learning ICEL2011*, 23-24 November, Bandung, Indonesia. *Procedia - Social and Behavioral Sciences* Vol. 67, pp. 513 – 526

Raosoftware. Sample size calculator [Online]. Available:
<http://www.raosoftware.com/samplesize.html> [Accessed 5 March 2016].

Roschelle, J. M., Pea, R. D., Hoadley, C. M., Gordin, D. N., and Means, B. M. (2000) ‘Changing how and what Children learn in school with computer-based technologies’, *The Future of Children*, Vol. 10, No. 2, pp.76-101.

Roschelle, J. (2003) ‘Unlocking the learning value of wireless mobile devices’, *Journal of Computer Assisted Learning*, Vol. 19, No.3, pp.260-272.

Roschelle, J. (2003) ‘Unlocking the learning value of wireless mobile devices’, *Journal of Computer Assisted Learning* Vol. 19, No. 3, pp.260-272

Russello, G., Crispo, B., Fernandes, E., & Zhauniarovich, Y. (2011) ‘Yaase: Yet another android security extension. In privacy, security, risk and trust (PASSAT)’, *IEEE Third International Conference on Social Computing (SocialCom)*, pp. 1033-1040.

Saunders, M., Lewis, P., Thornhill, A and Thill, J, V. (2012). *Research Methods for Business Students*. 6th Edition. Pearson Education Ltd, England

Selim, H. M. (2007) ‘Critical success factors for e-learning acceptance: confirmatory factor models’, *Computers & Education*, Vol. 49, No. 2, pp. 396–413.

Sharples, M. (2013) Mobile learning: research, practice and challenges. *Distance Education in China*, Vol. 3, No.(5), pp.5-11.

Sharples M., Milrad M., Arnedillo Sánchez, I and Vavoula G. (2009) Mobile learning: Small devices, big issues in Balacheff, N., Ludvigsen, S. et al. (eds) *Technology-Enhanced Learning: Principles and Products*, Heidelberg, Germany: Springer, pp. 233-249

Shabtai A., Kanonov U., Elovici Y., Glezer C. and Y. Weiss,(2012). ‘Andromaly: a behavioural malware detection framework for android devices’, *Journal of Intelligent Information Systems*, Vol. 38, No.1, pp.161-190

Shonola, S. A and Joy, M.S (2015) ‘Security of m-learning System: A collective responsibility’, *International Journal of Interactive Mobile Technologies (iJIM)* pp.64 – 70 <http://dx.doi.org/10.3991/ijim.v9i3.4475>

Shonola, S.A and Joy, M.S. (2014), 'Investigating Attack Vectors in M-learning Systems in Nigerian Universities', *International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, 13-14 November 2014, Thessaloniki, Greece

Shonola, S. A and Joy, M.S (2014) 'Mobile learning security concerns from university students' perspectives", *8th International Conference on Interactive Mobile Communication Technologies and Learning, Thessaloniki, Greece*. pp. 165-172 <http://dx.doi.org/10.1109/imctl.2014.7011125>

Shonola, S. A and Joy, M.S (2014) 'Security framework for mobile learning environments', *Proceedings of ICERI2014 Conference* 17th-19th November 2014, Seville, Spain

Shonola, S. A and Joy, M.S (2014) 'Learners' perception on security issues in m-learning (Nigerian Universities case study)', *Exchanges: The Warwick Research Journal*, Vol. 2, No. 1, pp. 107 – 128

Smith, J.A. ed. (2015) *Qualitative psychology: A practical guide to research methods*. Sage.

Somekh, B. and Lewin, C. (2005) *Research methods in the social sciences*, London: Sage.

Southworth, J.H., Flanigan, J.M., and Knezek, G (1981) 'Computers in education: international multi-mode electronic conferencing', *The Printout*: pp. 8-13.

Staron, M. (2007) 'Using experiments in software engineering as an auxiliary Tool for teaching--A qualitative evaluation from the perspective of students' learning process', In: *29th international conference on Software Engineering* Minneapolis, USA.

Szajna, B. (1996) 'Empirical evaluation of the revised technology acceptance model', *Management Science*, Vol. 42, No.1, pp. 85-92.

Szucs, A. (2009) 'New horizons for higher education through e-learning'. Available from www.elearningpapers.eu [Accessed on 05 October 2014]

Symantec (2008) *Symantec Internet Security Threat Report: Trends for July–December 2007*

Taleb. Z and Sohrabi, A (2012) 'Learning on the move: the use of mobile technology to support learning for University Students', *International Conference on Education & Educational Psychology*, *Procedia Social and Science Behaviour*. Vol.69, pp. 1102 – 1109.

- Tarle, P.R. (2015) 'Comparative Study of Smart Phone Security Techniques', *International Journal of Emerging Technology and Advanced Engineering*, Vol 5, No.2.
- Taylor, S.J., Bogdan, R. and DeVault, M (2015) *Introduction to qualitative research methods: A guidebook and resource*. John Wiley & Sons.
- Terras, M and Ramsay, J (2012) 'The five central psychological challenges facing effective mobile learning', *British Journal of Educational Technology*, Vol.43, No.5, pp.820 – 832
- The Scoop, The top 10 most populated universities in Nigeria. Available online <http://www.thescoopng.com/the-top-10-most-populated-universities-in-nigeria/> [accessed on 30 Jun 2016]
- Traxler, J. (2010) Students and mobile devices: choosing which dream. Research in Learning Technology
- Traxler, J. and Koole, M. (2014). The Theory Paper: What Is the Future of Mobile Learning?. *International Association for Development of the Information Society*.
- Travis, D (2011) 'ISO 13407 is dead. Long live ISO 9241-2101 Available on <http://www.userfocus.co.uk/articles/iso-13407-is-dead.html> Accessed on [27- June-2016]
- Traxler, J. and Vosloo, S (2014) 'Introduction: The prospects for mobile learning', *Prospects*, Vol. 44, No.1, pp.13-28
- Tupakula, U and V. Varadharajan (2013) 'Security techniques for counteracting attacks in mobile healthcare services', *The 3rd International conference on current and future trends of information and communication technologies in healthcare (ICTH-2013)*. Procedia Computer Science, vol. 21, pp. 374 – 81
- Tugui. O., Funar. S. and Cofari, A (2008) 'Trends of integrating the e-learning platform in the graduate agronomic educational system in Romania', *Bulletin of University of Agricultural Sciences and Veterinary Medicine Cluj-Napoca, Horticulture*, Vol. 65, No.2, pp.621-626
- Udanor, C.N. and Nwodoh,A.T (2010). 'A Review of M-learning Models' *Indian Journal of Computer Science and Engineering*, Vol.1, No. 4, pp. 426-436.
- Uden, L. (2007). 'Activity Theory for Designing Mobile Learning', *Journal of Mobile Learning and Organisation*, Vol.1, No.1, pp. 81-102

Van Ruitenbeek, E., Courtney, T., Sanders, W. H., and Stevens, F. (2007) 'Quantifying the effectiveness of mobile phone virus response mechanisms', *In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 790-800

Van Velsen, L., Van Der Geest, T., Klaassen, R. and Steehouder, M (2008) 'User-centered evaluation of adaptive and adaptable systems: a literature review', *The knowledge engineering review*, Vol.23, No.3, pp. 261-281.

Venkatesh, V. and Davis, F. D. (2000) 'A theoretical extension of the technology acceptance model: Four longitudinal field studies', *Management Science*, Vol. 46, No.2, pp. 186-204.

Vinekar, V., Slinkman, C. and Nerur, S. (2006) 'Can agile and traditional systems development approaches coexist? An ambidextrous view. *Information Systems Management*, Vol.23, No.3, pp.31-42.

Vogel D., Kennedy D. & Kwok R.C.-W (2009) 'Does using mobile device applications lead to learning?', *Journal of Interactive Learning Research* Vol. 20, pp.469–485

Wallace, L.G. and Sheetz, S.D., 2014. The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management*, Vol. 5, No.2, pp.249-259.

Walker, K. (2007). 'Introduction: Mapping the Landscape of Mobile Learning.' In M. Sharples (Ed.), *Big Issue in Mobile Learning: a Report of a New Workshop by the Kaleidoscope Network of Excellence Mobile Learning Initiative* (pp. 5-6), UK: Learning Science and Research Institution: University of Nottingham.

Waziri, K. M. (2011) 'Intellectual Property Piracy and Counterfeiting in Nigeria: The Impending Economic and Social Conundrum', *Journal of Politics & Law*, Vol.4, No.2, pp.196-202

Welsh, E. T., Wanberg, C. R., Brown, K. G. and Simmering, M. J. (2003), 'E-learning: emerging uses, empirical results and future directions', *International Journal of Training and Development*. Vol. 7, No.4, pp. 245–258

WENR (2013) Education in Nigeria 'World Education News and Reviews' Available online <http://wenr.wes.org/2013/07/an-overview-of-education-in-nigeria> published on July 1, 2013. Accessed on [30 Jun 2016]

Wu, B. and Zhang, C. (2014) 'Empirical study on continuance intentions towards E-Learning 2.0 systems', *Behaviour & Information Technology*, Vol.33, No.10, pp.1027-1038.

Wu, B., Xu W., and Ge, J.(2012) ‘Innovation research in e-Learning’, *A paper presented at International Conference on Applied Physics and Industrial Engineering*. Physics Procedia, Vol. 24, pp. 2059 – 2066

Wu, W-H., Wu Y-C, J., Chen, C-Y., Kao, H-Y., Lin C-H and Huang, S-H. (2012) ‘Review of trend from mobile Learning studies: A meta-analysis’, *Computers & Education* Vol. 59 (2012), pp. 817–827

Yaiparaj, S., Harmantzis, F., and Gunasekaran, V (2008). ‘On the economics of GPRS networks with Wi-Fi integration’, *European Journal of Operational Research*, Vol. 187, No. 3, pp. 1459-1479

Yang, H.H.(2010) ‘New world, new learning: Trends and issues of e-Learning’ *Procedia - Social and Behavioral Sciences*. Vol. 77 (2013), pp. 429 – 442.

Yap, T.S and Ewe, H. T (2005) ‘A mobile phone malicious software detection model with behavior checker: web and communication technologies and internet-related social issues’, *Springer Berlin Heidelberg*, Vol. 359, pp.57- 65.

Yengin, I., Karahoca, D., Karahoca, A and Ozcinar, Z (2010) ‘Being ready for the paradigm shifts in e-learning: Where is the change happening and how to catch the change?’ *Procedia Social and Behavioral Sciences* Vol. 2, pp. 5762–5768

Zafar, A., Hasan, S. and Trigui, M (2014) Towards secure m-Learning: An analysis (pp. 148-159). *MAGNT Research Report*, Vol. 2 No.5.

Zamzuri, Z. F., Manaf, M., Yunus, Y., and Ahmad, A. (2013) ‘Student perception on security requirement of e-learning services’, *Procedia-Social and Behavioral Sciences*. Vol. 90 (2013), pp.923-930.

Zhang, D., Zhao, J. L., Zhou, L., and Nunamaker, J. F. (2004). ‘Can e-learning replace classroom learning?’ *Communications of the ACM*, Vol. 47, No. 5, pp.74–7

Zhang, D., and Nunamaker, J. F. (2003), ‘Powering e-learning in the new millennium: an overview of e-learning and enabling technology’, *Information Systems Frontiers*, Vol. 5, No.2, pp.207– 218.

Appendix 1

First Research Questionnaire

Secure Mobile Learning

Questionnaire

My name is Adekunle Shonola. I am a PhD student at The University of Warwick, UK and I am researching on security issues in mobile learning. The purpose of this questionnaire is to explore students' awareness of secure mobile learning and to get information on it. Please be aware that your participation is voluntary and the data collected will be totally confidential and will be stored in an anonymous manner. Also note that the Department's ethical rules and procedures have been followed, and ethical consent has been granted for this questionnaire.

Section 1: Personal Information & Demographics

Please complete this questionnaire carefully and for any clarification contact me at S.A.Shonola@warwick.ac.uk

Name (optional): _____

College/University: _____

Year of Study: _____

Department: _____

Course: _____

What is your age? (Please tick one)

- ☐ Under 20
- ☐ 20 - 25

- 26 and over
- Prefer not to say

What is your gender? (Please tick one)

- Female
- Male

Section 2: Mobile Devices

NOTE: *For the purpose of this research work, mobile device includes any of the following; Mobile Phone, Smart Phone, Tablet, eReader and MP3 Player.*

1. What kind of mobile devices (s) do you have? (Please tick all that apply)

- ☐ Mobile Phone (Not a Smart phone)
- ☐ Smart Phone
- ☐ Tablet
- ☐ eReader (e.g. Kindle)
- ☐ MP3 Player
- ☐ Other (please specify) _____

2. Which activities do you use your mobile device for? (Please tick all that apply)

- ☐ Phone calls
- ☐ Reading
- ☐ Video Conferencing
- ☐ SMS/MMS (texting)
- ☐ Games/Entertainment
- ☐ Internet access (browsing)

☐ Other (please specify) _____

3. Do you use your mobile device when you are at this place(s)? (Please tick all that apply)

☐ College / University

☐ Home

☐ Work

☐ In Transit

☐ Park / Playground

☐ Other (please specify) _____

4. How often do you download or install apps on your mobile device? (Please tick one)

☐ Very Often

☐ Often

☐ Rarely

☐ Occasionally

☐ Never

Section 3: Mobile Learning

NOTE: *Mobile Learning is the use of mobile devices (e.g. mobile phones, smartphones and tablets) for learning purposes.*

5. Are you aware that mobile devices are widely used in Colleges/Universities for learning purposes?

☐ Yes

- No

6. Have you used your mobile device for any of these learning activities? (Tick all that apply)

- ☐ Studying course materials
- ☐ Searching for additional course materials
- ☐ Online Assessment
- ☐ Group discussion
- ☐ Others (please specify) _____

7. Does having course materials such as slides and lecture notes on your mobile will improve your learning skills? (Please tick one)

- Completely Agree
- Somewhat Agree
- Neither Agree nor Disagree
- Somewhat Disagree
- Completely Disagree

8. On a scale of 1-5 (1=extremely important, 2=moderately important, 3=somewhat important, 4=slightly important, 5=not at all important), rate how important each of the following activities is to you when using your mobile device for educational purposes (Please tick one circle on each row).

| Activities | 1 | 2 | 3 | 4 | 5 |
|-----------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Taking notes in the class | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Downloading course material | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | | | | |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Studying and Researching | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Completing online exercises | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Lecturers sharing materials & information | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Communicating outside classroom with my lecturers and fellow students | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Receiving grades and feedback through email | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

9. Does using your mobile device for learning will improve your performance in your courses? (Please tick one)

- ☐ Completely Agree
- ☐ Somewhat Agree
- ☐ Neither Agree nor Disagree
- ☐ Somewhat Disagree
- ☐ Completely Disagree

10. Do you want to use or continue to use mobile device for learning on a regular basis?

- ☐ Yes
- ☐ No

Please give a reason

Section 4: Mobile Learning Security

NOTE: For the purpose of this research work, Mobile security is safeguarding of mobile device from theft and protection of its contents and data from unauthorised access and manipulation.

11. How important is the security of your mobile device to you? (Please tick one)

- ☐ Very important
- ☐ Important
- ☐ Neither important nor unimportant
- ☐ Not Important
- ☐ Not Important at all
- ☐ I'm not sure

12. Has the security of your mobile device been breached before?

- ☐ Yes
- ☐ No

If no, go to question 14.

13. How was the security of your mobile device breached? (Tick all that apply)

- ☐ Through mobile web browser
- ☐ No password lock
- ☐ Bluetooth sharing was left on
- ☐ Email access / attachment
- ☐ Downloads from unknown source
- ☐ Others (please specify) _____

14. What are the security concerns students may have when using mobile devices for learning? (Tick all that apply)

- ☐ Theft of mobile device
- ☐ Virus / Malware attack
- ☐ Unauthorised access to mobile device
- ☐ Denial of Service
- ☐ Others (please specify) _____

15. What are the security concerns lecturers may have when using mobile devices for teaching? (Tick all that apply)

- ☐ Students exploiting a security breach
- ☐ Data Interception
- ☐ Virus /Malware attack
- ☐ Denial of Service
- ☐ Unauthorised access to materials
- ☐ Propagation of false or misleading information
- ☐ Others (please specify) _____

16. What do you think are the damaging effect(s) of mobile learning security threats to the students? (Tick all that apply)

- ☐ Loss of confidential information
- ☐ Loss of study hours (e.g. due to downtime)
- ☐ Loss of performance
- ☐ Psychological damage
- ☐ Others (please specify) _____

17. What do you think are the damaging effect(s) of mobile learning security threats to the lecturers? (Tick all that apply)

- ☐ Loss of confidential information
- ☐ Loss of control (e.g. over online assessment)
- ☐ Loss of content quality
- ☐ Psychological damage
- ☐ Others (please specify) _____

18. What do you think are the damaging effect(s) of mobile learning security threats to the Higher Education Institution? (Tick all that apply)

- ☐ Loss of confidential information
- ☐ Loss of goodwill / integrity
- ☐ Loss of reliability
- ☐ Loss of person's hours
- ☐ Others (please specify) _____

19. Who among the stakeholders in m-learning are affected most by any security threat?

- ☐ Students
- ☐ Lecturers/Support Staff
- ☐ Management/promoters
- ☐ Developers/Admin

20. Which component of an m-learning system you think is commonly attacked?

- ☐ Mobile devices
- ☐ M-learning servers (web, apps, database)
- ☐ Network devices

21. How do you think the mobile learning security threats or issues are assessed?
(Tick all that apply)

- ☐ Report by users of unusual behaviour of device
- ☐ System monitoring /Alert
- ☐ Log file analysis
- ☐ Frequency of service denial due to virus / malware attack
- ☐ Others (please specify)

22. How do you think the mobile learning security threats can be minimised?
(Tick all that apply)

- ☐ Biometric features
- ☐ Device password lock
- ☐ Data encryption
- ☐ Remote wipe of data after device loss
- ☐ Device location track
- ☐ Data Backup
- ☐ Regular antivirus / anti malware updates
- ☐ Cloud storage of materials (e.g. Dropbox)
- ☐ Others (please specify)

23. Apart from security issues mentioned earlier, are you aware of any other security concerns that are peculiar to Nigeria Higher Education system in relation to mobile learning?

- ☐ Yes
- ☐ No

If yes, please specify

End of questionnaire

Thank you for participating in this survey

Appendix 2

First Research Interview

INTERVIEW SURVEY FOR INSTRUCTORS AND TECHNICAL STAFF

DATE/TIME:.....

INTERVIEWEE NAME:.....

POSITION:.....

DEPARTMENT:.....

INSTITUTION NAME:

Note: Interviewee has the rights to remain anonymous

QUESTION 1:

Are you aware of emerging m-learning in higher education institutions?

.....

.....

.....

.....

QUESTION 2:

It has been shown that m-learning is suited for informal education, how do you think m-learning can be adapted for formal education?

.....

.....

.....

.....

QUESTION 3:

As a Lecturer/Technical staff, do you support the use of m-learning or the use of mobile devices as an education tool in higher institutions in Nigeria? If yes why?

.....

.....

.....

.....

QUESTION 4:

Which area do you think m-learning is more useful for, teaching aid or assessment? And why?

.....

.....

.....

.....

QUESTION 5:

Do you know if the university management is willing to adopt or implement m-learning to complement classroom teaching?

.....

.....

.....

.....

QUESTION 6:

Do you know of any threat including security that might affect the implementation of m-learning in higher institutions in Nigeria? If so, what?

.....

.....

.....

.....

QUESTION 7:

Are you aware of any mobile security concerns that lecturers may have when using mobile devices as a teaching aid in higher institutions in Nigeria? If so, what are the issues and how does it affect them?

.....

.....

.....

.....

QUESTION 8:

Which component of an m-learning system you think is commonly attacked and how?

.....

.....

.....

.....

QUESTION 9:

What are the considerations for deployment of m-learning, mostly in relation to security aspects?

.....

.....

.....

.....

QUESTION 10:

Who among the stakeholders in m-learning are affected most by any security threat?

.....

.....

.....

.....

QUESTION 11:

Who do you think is responsible for ensuring risk free m-learning in higher education institutions in Nigeria?

.....

.....

.....

.....

QUESTION 12:

How can these security concerns that affect m-learning be assessed?

.....

.....

.....

.....

QUESTION 13:

How can these security threats to m-learning be overcome in higher institution in Nigeria?

.....

.....

.....

.....

QUESTION 14:

What are other threats apart from mobile security, such as political or legal, facing m-learning in Nigeria?

.....

.....

.....

.....

QUESTION 15:

Apart from security issues mentioned earlier, are you aware of any other security concerns that are peculiar to Nigeria education system in relation to m-learning?

.....

.....

.....

.....

QUESTION 16:

What possible solutions do you have for the circumstances you have mentioned after the previous question, if any?

.....

.....

.....

.....

End of interview

Thank you for participating in this survey

Appendix 3

Frameworks Interview

FRAMEWORK EVALUATION INTERVIEW QUESTIONS

The purpose of these interview questions is to evaluate the m-learning security frameworks which the researcher has previously or just discussed with you.

Demography:

- Gender: (i) Male (ii) Female
- Age group: (i) 20 – 29 (ii) 30 – 39 (iii) 40 – 49
(iv) 50 – 59 (v) Over 60
- Status: (i) PG Student (ii) Lecturer (iii) Academic
(iv) Support Industrialist

Framework Questions:

- 1) What is your background? Do you have any experience with mobile security?
- 2) Do you think there is a need for m-learning security framework and why?
- 3) What is your view on the proposed m-learning security framework?
- 4) Does the framework conform to relevant standards?
- 5) Do you think it is necessary to have the sub-frameworks along with the main framework and why?
- 6) Which of the sub-framework do you think is most relevant to m-learning and why?

- 7) Do you think the framework and sub-frameworks address all known security issues and concerns?
- 8) Do you think the framework and sub-frameworks are fit for purpose? State why?
- 9) Do you think developing the frameworks are necessary in solving m-learning security issues in Nigerian HEIs? State your reasons.
- 10) Do you have any suggestion on improving the features of the framework? If yes, what are the suggestions?

Thank you for your time.

Appendix 4

Enhancement App Questionnaire

Please complete this questionnaire carefully and for any clarification contact me at S.A.Shonola@warwick.ac.uk

Section 1: Mobile Device Security

1. Which mobile device do you use? (Please tick all that apply)
 - ☐ Android (Smartphone, tablet)
 - ☐ Apple (Smartphone, tablet)
 - ☐ Microsoft (Surface)
 - ☐ Other (please specify) _____
2. Do you have notes, tips or information on how to keep your mobile device safe?
 - ☐ Yes
 - ☐ No
3. If yes, where/how do you get the tips or information from? (Please tick all that apply)
 - ☐ Device manual
 - ☐ Internet (e.g. manufacturer's site)
 - ☐ Lectures notes
 - ☐ Word of mouth
 - ☐ Other (please specify) _____
4. Have you had any security awareness tutorial or seminar on keeping mobile device safe before?
 - ☐ No

- Yes
5. Due to increasing usefulness of mobile device for learning, do you think it is important to have extra lecture or seminar on mobile device security?
- No
 - Yes
6. Do you have any security app such as anti-virus installed on your mobile device?
- No
 - Yes

Section 2: M-learning Security App

NOTE: Please download and use the m-learning security awareness app before continuing

7. Do you understand the use or purpose of the m-learning security enhancement app?
- Yes
 - No

If you answer no, please contact the undersigned.

8. How do you think the enhancement app is useful to you? (Tick all that apply)

- ☐ It gives me new tips and information on keeping my device safe
- ☐ It reminds me on how to keep my device safe
- ☐ The vulnerability scan on the app solve some security issues for me
- ☐ The scan notification is timely
- ☐ The reporting section is precise and useful

9. On a scale of 1-5 (1=lowest and 5=highest), rate the app in terms of: (Please tick one circle on each row).

| Activities | 1 | 2 | 3 | 4 | 5 |
|-------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Easy to use | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | | | | |
|---------------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Improve your security awareness | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Enhance security of your device | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Contribute to your security knowledge | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Fit for purpose | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

10. On a scale of 1-5 (1=lowest and 5=highest), evaluate each section of the app:
(Please tick one circle on each row).

| Sections | 1 | 2 | 3 | 4 | 5 |
|------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Limiting unauthorised access | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Avoiding malware | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Learning content security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Free Wi-Fi concern | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Unusual device behaviour | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Bluetooth concern | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Browsing securely | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Regular updates | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security tips summary | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security scan report | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

11. Have you experienced any security issue on your m-learning device before?

- ☐ Yes
- ☐ No

12. Does the app addresses the security issue?

- ☐ Yes
- ☐ No

If No, Please state:

13. List the positive aspects/features of m-learning security app

- 1.
- 2.
- 3.

14. List any negative aspects of m-learning security app

- 1.

- 2.
- 3.

15. List any other features you would like to see in m-learning security app

- 1.
- 2.
- 3.

16. Has your security awareness on m-learning has improved due to the use of the app?

- ☐ Yes
- ☐ No

17. Does this security enhancement app meets your expectation?

- ☐ Yes
- ☐ No
- ☐ Not sure

18. Do you want to continue using the security enhancement app in future?

- ☐ Yes
- ☐ No
- ☐ Not sure

End of questionnaire

Thank you for participating in this survey

Appendix 5

Enhancement App Interview

EVALUATION INTERVIEW QUESTIONS

Demography:

- What is your Age group pls? (i) 20 – 29 (ii) 30 – 39 (iii) 40 – 49 (iv) 50 – 59
- Gender (i) Male (ii) Female

App Questions:

- Do you find the app installation easy and smooth? **What issues do you have during installation?**
- Have you tried using the app? **How many times do you tried the app?**
- Which section of the app do you find very useful in terms of security? **And why?**
- The app does awareness promotion, vulnerability scan and threat reporting, which area does it perform best? **And why?**
- Do you encounter any issue when using the app? If yes, what's the issue?
- Do you think the app could improve the security of your device? If yes in what area?
- Do you check the security report of the app from time to time for any identified security issue? **What is your observation?**
- Do you think the app is fit for purpose? **State why?**
- What is your general opinion on the app? **Why do you have such opinion?**
- Do you have any suggestion on improving the app?

Thank you for your time.